ANTIVÍRUS EMPRESARIAL

Manual de Utilização

Se ainda tiver dúvidas entre em contato com a equipe de atendimento:

Por telefone: 0800 642 3090

Por e-mail atendimento@oisolucoespraempresas.com.br

Índice

1. O que fazer após a instalação 6
2. Configurar meus programas de e-mail para filtrar spam 6
3. Como as minhas próprias regras de filtragem e de e-mail funcionam juntas? 6
4. Como me certificar de que o computador está protegido 6
5. O que o ícone da bandeja do sistema indica 7
6. Exibir o status geral da minha proteção 8
7. Como executar tarefas comuns 8
8. Abrir o produto 8
9. Abrir as configurações avançadas 9
10. Como utilizar os atalhos 9
11. Verificar no Windows Explorer 9
12. Executar tarefas a partir da bandeja do sistema 10
13. Como ver o que o produto fez 12
14. Exibir estatísticas 12
15. O que são notificações 13
16. O que é a Rede de proteção em tempo real 13
17. Declaração de privacidade 13
18. Proteção do meu computador contra malware 14
19. O que são vírus e outros tipos de malware 14
20. Vírus 15
21. Spyware 15
22. *Rootkits* 15
23. Riskware 16
24. Como verificar o meu computador 16
25. Verificar se há malware 17
26. A proteção em tempo real afeta o desempenho do computador? 17
27. Ativar a verificação em tempo real 17
28. Verificar se há malware no meu e-mail 18
29. Quando as mensagens de e-mail e anexos são verificados 18
30. Ativar e desativar a verificação do e-mail 19
31. Definir as portas usadas para diferentes protocolos de e-mails 19
32. Ativar a verificação do tráfego da web 20
33. Bloquear cookies de rastreamento 20
34. Verificar em horários definidos 20
35. Agendar uma verificação 21
36. Cancelar uma verificação agendada 21
37. Ver os resultados de verificação agendada 22
38. Verificar manualmente 23
39. Como selecionar o tipo de verificação manual 23
40. Tipos de verificação 23
41. Limpar malware automaticamente 25
42. Ver os resultados da verificação manual 25
43. Selecionar arquivos que serão verificados 26
44. Incluir arquivos 26

45. Excluir tipos de arquivo 27
46. Excluir arquivos de acordo com o local 28
47. Ver aplicativos excluídos 29
48. Verificar dentro de arquivos e pastas compactadas 30
49. Selecionar a ação quando algo for encontrado 30
50. Ações a realizar em caso de arquivos infectados 30
51. Ações padrão na verificação em tempo real 31
52. Ações padrão na verificação manual e agendada 31
53. Ações padrão para o DeepGuard 32
54. Ver histórico de vírus e spyware 33
55. O que é o DeepGuard? 33
56. Como o DeepGuard funciona 33
57. Como ativar o DeepGuard 34
58. Permitir programas que o DeepGuard bloqueou 34
59. Como desativar o monitoramento avançado de processos 35
60. Proteger contra alterações perigosas no sistema 35
61. Como ver o que o DeepGuard fez 37
62. Como utilizar a quarentena 37
63. Ver itens em quarentena 38
64. Restaurar itens da quarentena 39
65. Como utilizar as atualizações automáticas 39
66. Verificar o status da atualização 39
67. Alterar minhas configurações de conexão à internet 40
68. Verificar o status da Rede de proteção em tempo real 41
69. Ativar as atualizações automáticas 41
70. Segurança das conexões de rede 42
71. O que é um firewall 42
72. O que são perfis de firewall 43
73. Como os perfis de firewall estão relacionados a serviços e regras 44
74. Como alterar o perfil de firewall 44
75. O que são serviços e regras de firewall 44
76. O que são regras de firewall 45
77. Quando é necessário adicionar uma nova regra de firewall? 45
78. Ver regras de firewall 46
79. Detalhes da regra de firewall 47
80. O que são serviços de firewall 47
81. Ver serviços de firewall 48
82. O que são regras de firewall dinâmicas 49
83. Ver regras de firewall 49
84. Como funcionar a ordem de prioridade das regras de firewall 50
85. Um exemplo de como funciona a ordem de prioridade 50
86. Como permitir ou bloquear tráfego de rede por meio do firewall 51
87. O que fazer se um alerta do firewall for exibido 51
88. Ativar e desativar os alertas de firewall: 52
89. Como criar regras e serviços de firewall 52

90. Criar um serviço de firewall 52
91. Iniciar a criação de uma regra 54
92. Selecionar os endereços IP 55
93. Como posso definir uma sub-redeIP? 56
94. Selecione os serviços e direção: 56
95. Selecionar opções de alerta 57
96. Verificar e aceitar a regra 58
97. Definir a ordem de prioridade das regras de firewall 58
98. Como abrir uma porta por meio do firewall 58
99. Exemplos de criação de regras de firewall 59
100. Criar uma regra para jogo de rede 59
101. Criar uma regra para compartilhar arquivos em uma rede doméstica 60
102. Ativar e desativar uma regra de firewall 62
103. Alterar uma regra de firewall 62
104. Configurações do firewall 63
105. Alterar as configurações do IPv6 63
106. O que fazer se você compartilhar uma conexão à internet 64
107. E se eu usar uma placa de TV digital? 65
108. Como controlar aplicativos de rede 65
109. Qual é a diferença entre o firewall e o controle de aplicativos 66
110. O que fazer se uma janela pop-up do controle de aplicativos for exibida 67
111. Programas seguros e inseguros e tentativas de conexão 68
112. Quais programas e tentativas de conexão podem ser considerados seguros 68
113. Quais programas e tentativas de conexão podem não ser considerados seguros 68
114. Permitir ou negar conexões para programas: 68
115. Ativar e desativar pop-ups do controle de aplicativos 70
116. O que fazer se um programa parar de funcionar 70
117. Como evitar intrusos 71
118. Qual é a diferença entre o firewall e a prevenção de intrusão 72
119. Selecionar como tentativas de intrusão são resolvidas 72
120. Como controlar conexões discadas 73
121. O que fazer se uma janela pop-up do controle de discagem for exibida 73
122. Editar números de telefone permitidos 74
123. Ver programas que têm permissão para fechar conexões discadas 76
124. Ver tentativas de conexão discada 76
125. O que fazer se não conseguir acessar a internet 77
126. Onde encontrar alertas do firewall e arquivos de registro 77
127. Ver alertas do firewall 77
128. Informações sobre o alerta do firewall 78
129. Ver o registro de ações 79
130. Exemplos de registro de ações 79
131. Abertura de uma conexão 79
132. Recebimento de uma conexão 80
133. Adição e remoção de uma regra de firewall dinâmica 80
134. Monitorar tráfego de rede com registro de pacote 80

135. Como funciona o registro de pacote 80
136. Iniciar registro de pacote 81
137. Ver o registro de pacote 82
138. Uso da internet com segurança 83
139. O que é proteção durante a navegação 83
140. Como ativar ou desativar a proteção durante a navegação 84
141. Classificações de segurança da proteção durante a navegação 85
142. Mostrar classificações de links da web 85
143. Como classificar sites 86
144. Proteger contra conteúdo perigoso 87
145. Permissão de acesso a sites confiáveis 87
146. Ativar ou desativar as proteções contra vulnerabilidades 88
147. O que fazer quando um site estiver bloqueado 88
148. Resumo de segurança de um site 89
149. Bloquear spam 90
150. Configurar meus programas de e-mail para filtrar spam 90
151. Como as minhas próprias regras de filtragem e de e-mail funcionam juntas? 91
152. Programas de e-mail da Microsoft 91
153. Limpar as pastas de lixo e phishing 91
154. Programas de e-mail Netscape e Mozilla Thunderbird 92
155. Criar pastas para mensagens de e-mail com spam e phishing 92
156. Criar regra de filtragem de spam 93
157. Criar regra de filtragem de phishing 94
158. Programa de e-mail Opera 94
159. Criar filtros para mensagens de e-mail com spam e phishing 95
160. Criar regra de filtragem de spam 95
161. Criar regra de filtragem de phishing 96
162. Programa de e-mail Eudora 97
163. Criar pastas para mensagens de e-mail com spam e phishing 97
164. Criar regra de filtragem de spam 97
165. Criar regra de filtragem de phishing 98
166. E se eu receber um monte de spam 98
167. Quais são os níveis de spam e phishing 99
168. Alterar o nível de filtragem de spam e phishing 100
169. Redefinir sistema de aprendizagem de spam e phishing 100
170. Definir a porta para protocolos de e-mail 101
171. Permitir e bloquear mensagens de endereços de e-mail específicos 101
172. Editar endereços de e-mail em que confio 101
173. Importar contatos para a minha lista de remetentes seguros 102
174. Bloquear mensagens de endereços de e-mail específicos 103
175. Proteger contra tentativas de phishing 104

1. O que fazer após a instalação

Após a instalação do produto, pode ser preciso configurar o cliente de e-mail e o navegador da web para funcionar com o produto.

2. Configurar meus programas de e-mail para filtrar spam

É possível criar uma pasta de spam, de phishing e regras de filtragem em seu programa de e-mail para filtrar spam.

A filtragem de e-mail cria uma pasta de spam e de phishing e as regras de filtragem automaticamente no Microsoft Outlook, Microsoft Outlook Express e no Windows Mail (no Windows Vista). Se você usar algum outro programa de e-mail, deverá criar as pastas e as regras de filtragem manualmente. Se você tiver várias contas de e-mail, crie as regras de filtragem para cada conta separadamente.

Nota: A filtragem de spam e phishing suporta apenas o protocolo POP3. Os programas de e-mail baseados na web ou outros protocolos não são suportados.

3. Como as minhas próprias regras de filtragem e de e-mail funcionam juntas?

A filtragem de e-mail filtra as mensagens de e-mail com base nas suas próprias regras de filtragem. Ele não filtra mensagens de e-mail que correspondam a uma regra que você tenha criado. Se você criou, por exemplo, uma regra que filtra todas as mensagens de e-mail de um armazenamento da web para a pasta Armazenamento da web, tanto as mensagens de confirmação de ordem quanto o material de propaganda desse Armazenamento da web serão movidos da sua caixa de entrada e filtrados para a pasta Loja da web.

4. Como me certificar de que o computador está protegido

É possível verificar o ícone de status na bandeja do sistema e o status do produto na página Status atual para certificar-se de que o computador está protegido.

5. O que o ícone da bandeja do sistema indica

Coloque o ponteiro do mouse sobre o ícone de status do produto na bandeja do sistema do Windows para exibir uma dica de ferramenta que mostra o status atual do produto.

Ícones de status e seus significados:

Ícone	Status	O que fazer
	O produto está funcionando corretamente. O computador está protegido.	Use o computador normalmente.
	O download de um produto está em andamento, e o computador estará protegido assim que o dowload for concluído.	O produto está fazendo download e instalando as atualizações mais recentes. Aguarde a conclusão do download.
	Ocorreu um erro, e o seu computador não está totalmente protegido.	Coloque o ponteiro do mouse sobre o ícone de status para ver o motivo do erro. Se necessário, reinicie o computador.
	Aviso! Um recurso do produto está desativado ou o produto está desatualizado. O computador não está totalmente protegido.	Coloque o ponteiro do mouse sobre o ícone de status para ver a dica de ferramenta de status. Ative o recurso que está desativado no momento ou verifique as atualizações do produto. **Nota:** Você pode ver esse ícone, por exemplo, se estiver desfragmentando o disco rígido, uma vez que algumas funções do sistema podem provocar a suspensão de downloads.
	Aviso crítico! O produto não está atualizado.	As *definições de vírus e spyware* não foram atualizadas ultimamente. Atualize as *definições de vírus e spyware* assim que for possível.
	O produto foi descarregado, e o computador não está protegido.	Clique com o botão direito do mouse no ícone de status e selecione Recarregar produtos do Oi para ativar o produto.
Nenhum ícone	O produto não está instalado ou algum erro impediu a inicialização do produto.	Reinicie o computador. Se o ícone não for exibido, reinstale o produto.

6. Exibir o status geral da minha proteção

A página Status mostra uma visão geral rápida dos recursos do produto instalados e os respectivos status no momento.

Para abrir a página Status: Na página principal, clique em Status.

A página Status é aberta.

Os ícones mostram o status do programa e seus recursos de segurança.

Ícone de status	Nome do status	Descrição
	OK	O computador está protegido. O recurso está ativado e funcionando adequadamente.
	Informações	O produto informa a respeito de um status especial de um recurso. O ícone é mostrado, por exemplo, quando um recurso é atualizado.
	Aviso	O computador não está totalmente protegido. Por exemplo, as definições de vírus podem estar desatualizadas, ou o status de um recurso requer atenção. Além disso, o firewall pode ser configurado para bloquear todo o tráfego da internet.
	Erro	O computador não está protegido Por exemplo, sua assinatura expirou, um recurso crítico está desativado ou o produto está em estado de erro. Além disso, o firewall pode ser configurado para permitir todo o tráfego.
	Desativado	Um recurso não crítico está desativado.

7. Como executar tarefas comuns

É possível ver os que pode ser feito com o produto e executar tarefas comuns na página Tarefas.

Para abrir a página Tarefas: Na página principal, clique em Tarefas.

A página Tarefas é aberta.

8. Abrir o produto

Clique duas vezes no ícone do status do produto na bandeja do sistema do Windows para abrir o produto.

Para abrir o produto:

a. Selecione uma das seguintes opções:
   - No Windows XP ou Vista: clique no ícone Mostrar ícones ocultos para mostrar os ícones da bandeja do sistema.
   - No Windows 7: clique no acento circunflexo para mostrar os ícones da bandeja do sistema.

b. Clique duas vezes no ícone .

A exibição principal é aberta e mostra o status atual da proteção.

Dica: É possível abrir o produto e a ajuda também a partir do menu Iniciar do Windows ou do ícone da área de trabalho do produto.

9. Abrir as configurações avançadas

Edite as configurações avançadas para alterar a maneira em que o produto funciona.

Para abrir as configurações avançadas:

Na página principal, clique em Configurações.

A janela Configurações é aberta.

O painel esquerdo lista os componentes do produto agrupados por suas funções. É possível alterar as configurações do produto no painel direito.

10. Como utilizar os atalhos

É possível verificar arquivos e pastas no Windows Explorer e executar diversas tarefas com o menu do ícone da bandeja do sistema.

11. Verificar no Windows Explorer

É possível verificar discos, pastas e arquivos em busca de vírus, spyware e *riskware* no Windows Explorer.

Para verificar um disco, pasta ou arquivo:

a. Coloque o ponteiro do mouse e clique com o botão direito no disco, pasta ou arquivos que você deseja verificar.

b. No menu que é exibido quando você clica com o botão direito do mouse, selecione Verificar se há vírus nas pastas. (O nome da opção depende do que está sendo

verificado: um disco, uma pasta ou um arquivo). A janela Assistente de Verificação é aberta e a verificação é iniciada.

Se um vírus ou um spyware for encontrado, o Assistente de Verificação levará você pelas etapas de remoção.

12. Executar tarefas a partir da bandeja do sistema

Você pode usar o ícone de status do produto localizado na bandeja de sistemas do Windows para executar as tarefas mais comuns com rapidez.

Para executar as tarefas:

a. Selecione uma das seguintes opções:
   - No Windows XP ou Vista: clique no ícone Mostrar ícones ocultos para mostrar os ícones da bandeja do sistema.
   - No Windows 7: clique no acento circunflexo para mostrar os ícones da bandeja do sistema.

b. Clique com o botão direito do mouse no ícone . Será aberto um menu com as tarefas mais comuns.

c. Selecione no menu a tarefa que você deseja executar.

Tarefas gerais:

Opção	O que faz
Abrir	Abre a interface do usuário do produto, onde você poderá ver o status de todos os componentes e acessar as configurações do produto para alterar o nível de proteção.
Mostrar lista de notificações	Exibe uma lista de mensagens de informação exibida pelo produto. Por exemplo, a lista inclui: ○ Eventos do Controle do sistema ○ Eventos da Verificação do tráfego da web ○ Itens das Notícias do serviço ○ Eventos da Verificação agendada
Suspender todos os downloads e atualizações	Caso esteja utilizando uma conexão com a internet que é cobrada pela quantidade de dados transferidos, é possível cancelar todos os downloads e atualizações.

Tarefas no submenu Verificação de vírus e *spyware*:

Opção	O que faz
Escolher o que verificar...	Verifica um arquivo ou pasta específica em busca de *vírus*, *spyware* e *riskware*. Selecione o diretório ou arquivo de destino e clique em OK para iniciar a verificação.
Varrer discos rígidos	Verifica todos os arquivos nas unidades de disco rígido para procurar *vírus*, *spyware* e *riskware*.
Verificação de vírus e spyware	Verifica o sistema para procurar *malware* e *riskware*.
Verificação de rootkit	Verifica o sistema para procurar *rootkits* e outros itens suspeitos e *ocultos*.
Verificação completa do computador	Verifica o computador para procurar *vírus*, *spyware* e *rootkits*.

Tarefas no submenu Conexões de rede:

Opção	O que faz
Bloquear todo o tráfego da rede	Bloqueia todo o tráfego de rede. Essa opção deve ser usada somente se você suspeitar que o computador esteja sendo atacado através da rede.
Permitir todo o tráfego da rede	Permite que todo o tráfego de rede passe. Essa opção desativa o firewall completamente e torna o computador vulnerável a todos os ataques através da rede.
Mostrar registro de alertas	Abre a caixa de diálogo Alertas do firewall.

Tarefas no submenu Filtragem de e-mail:

Opção	O que faz
Permitir remetente	Abre uma caixa de diálogo em que é possível adicionar o endereço de e-mail de um remetente à lista Remetentes permitidos. Essa lista contém os endereços que jamais serão filtrados para a pasta de spam.
Bloquear remetente	Abre uma caixa de diálogo em que é possível adicionar o endereço de e-mail de um remetente à lista Remetentes negados. Essa lista contém os endereços que serão filtrados para a pasta de spam.
Configurar filtragem	Abre as configurações de Filtragem de e-mail.

Opção	O que faz
de e-mail	

Submenu Sobre:

Opção	O que faz
Sobre	Mostra informações sobre o produto, por exemplo, o número da versão.

13. Como ver o que o produto fez

A página **Estatísticas** exibe o que o produto fez e você pode visualizar as ações que o produto realizou para proteger o computador no histórico de notificações.

14. Exibir estatísticas

É possível ver o que o produto fez desde a sua instalação na página Estatísticas.

Para abrir a página **Estatísticas**: Na página principal, clique em Estatísticas.

A página **Estatísticas** é aberta.

- A opção Última verificação de atualização realizada com êxito mostra o horário da última atualização.
- A opção Assinatura válida até mostra quando a assinatura atual irá expirar.
- A opção Verificação de vírus e spyware mostra quantos arquivos o produto verificou e limpou desde a instalação.
- Programas mostra quantos programas o DeepGuard permitiu ou bloqueou desde a instalação.
- A opção Verificação de e-mails mostra o número de anexos de e-mail válidos e o número de anexos que o produto limpou.
- A opção Filtragem de e-mail mostra quantas mensagens de e-mail o produto detectou como válidas e quantas foram detectadas como spam.

15. O que são notificações

Notificações são pequenos lembretes exibidos no canto inferior direito da tela do computador.

As notificações informam sobre as ações que o produto realizou para proteger o computador. O produto informa com notificações, por exemplo, quando ele bloqueia a inicialização de um programa potencialmente perigoso. Essas notificações são informativas e não requerem nenhuma ação sua.

16. O que é a Rede de proteção em tempo real

A Rede de proteção em tempo real do Oi Antivírus Empresarial é um serviço on-line que fornece respostas rápidas às ameaças vindas da internet.

A Rede de proteção em tempo real usa serviços de renome para obter informações sobre as ameaças mais recentes da internet. Você pode nos ajudar a desenvolver o serviço futuramente pela contribuição com informações detalhadas, como as fontes dos programas ou mensagens intrusas e a análise comportamental e estatística do uso do computador e internet.

Quando a caixa de seleção Sim, desejo participar da Rede de proteção em tempo real é selecionada na guia Privacidade, essas informações serão enviadas à Rede de proteção em tempo real.

Enviar informações à Rede de proteção em tempo real não compromete sua privacidade. Se desejar saber mais sobre o processamento das informações enviadas, leia nossa declaração de privacidade. Para fazer isso, clique em Leia nossa declaração de privacidade.

17. Declaração de privacidade

O envio de informações à Rede de proteção em tempo real não compromete sua privacidade.

Mesmo que as informações enviadas sejam consideradas pessoais em algumas jurisdições, sua privacidade é protegida durante o processo. Transferimos as informações com segurança, removemos todas as informações pessoais desnecessárias e processamos as informações anonimamente de maneira conjunta. Desse modo, as informações não são relacionadas a você de nenhuma maneira. Não

são incluídas nenhuma informação de conta de usuário, de endereço IP ou licença nas informações enviadas por meio da Rede de proteção em tempo real. Nós protegemos sua privacidade também pelo uso de criptografia na transferência das informações.
As informações enviadas são utilizadas para melhorar os recursos de proteção dos nossos serviços e produtos.

18. Proteção do meu computador contra malware

A verificação de vírus e spyware protege o computador contra programas que podem roubar informações pessoais, danificar o computador ou utilizá-lo para finalidades ilegais.
Quando qualquer tipo de malware for encontrado, por padrão eles são desativados imediatamente, antes que causem danos.
A verificação de vírus e spyware verifica os discos rígidos locais, qualquer mídia removível (como unidades portáteis ou CDs) e conteúdo baixado automaticamente por padrão.
Dependendo da configuração do produto, ele também verificará o e-mail e o tráfego da web. A verificação de vírus e spyware também observa o computador quanto a quaisquer alterações que possam indicar malware. Se quaisquer alterações perigosas do sistema, por exemplo, configurações do sistema ou tentativas de alterar processos importantes do sistema, forem encontradas, o DeepGuard interromperá a execução desse programa, pois é provável que seja um malware.

19. O que são vírus e outros tipos de malware

O malware é um programa especialmente criado para danificar o seu computador, usar o computador para objetivos ilícitos sem o seu conhecimento ou roubar informações do computador.
O malware pode:

- Controlar o seu navegador da web,
- Redirecionar suas tentativas de busca,
- Mostrar anúncios indesejados,
- Rastrear os sites que você acessa,
- Roubar informações pessoais, como suas informações bancárias,

- Usar seu computador para enviar spam e
- Usar seu computador para atacar outros computadores.

O malware também pode fazer com que o computador fique lento e instável. Você talvez suspeite que exista algum malware em seu computador se ele repentinamente tornar-se lento e travar com frequência.

20. Vírus

Geralmente, os vírus são programas que podem se anexar a arquivos e se multiplicar repetidamente; eles podem alterar e substituir os conteúdos de outros arquivos de modo a danificar o computador.

Um vírus é um programa que geralmente é instalado sem o seu conhecimento no computador. Depois de instalado, o vírus tenta multiplicar-se. O vírus:

- Usa alguns recursos do sistema do computador,
- Pode alterar ou danificar arquivos no computador,
- Provavelmente tenta usar seu computador para infectar outros computadores,
- Talvez permita que seu computador seja usado para objetivos ilícitos.

21. Spyware

Os *spywares* são programas que coletam suas informações pessoais.

Os *spywares* podem coletar informações pessoais, inclusive:

- Sites da internet que você acessou,
- Endereços de e-mail em seu computador,
- Senhas ou
- Números de cartões de crédito.

Os *spywares* quase sempre se instalam sem a sua permissão explícita. O spyware pode ser instalado junto com um programa útil ou enganando-o para clicar em uma opção em uma janela pop-up falsa.

22. *Rootkits*

Os *rootkits* são programas que dificultam a localização de outro malware.

Os *rootkits* ocultam arquivos e processos. Em geral, eles fazem isso para ocultar atividades maliciosas no computador. Quando um *rootkit* oculta um malware fica difícil descobrir se o computador tem um malware.

Este produto possui um scanner de *rootkit* que verifica especificamente a presença de rootkits, o que dificulta a ocultação do malware.

23. Riskware

O *riskware* não é desenvolvido especificamente para danificar o computador, mas ele pode danificá-lo se for mal utilizado.

O *riskware* não é exatamente um malware. Programas *riskware* executam algumas funções úteis, no entanto, potencialmente perigosas.

Exemplos de programas *riskware*:

- Programas para mensagens instantâneas, como o IRC (Internet Relay Chat),
- Programas para transferência de arquivos pela internet de um computador para outro,
- Ou programas de telefone pela Internet como o VoIP (Protocolo Voice over Internet).
- Softwares de acesso remoto, como o VNC.
- scareware, aqueles programas que podem tentar assustar ou enganar os usuários para que comprem software de segurança falso ou
- softwares projetados para burlar verificações de CD e proteções de cópias.

Se você explicitamente instalou o programa e o configurou corretamente, é menos provável que ele seja perigoso.

Se o *riskware* foi instalado sem o seu conhecimento, é bem provável que tenha sido instalado com intenções maliciosas e deverá ser removido.

24. Como verificar o meu computador

É possível verificar se há malware no computador em tempo real, manualmente, ou agendar uma verificação em horários definidos.

A decisão de que método utilizar depende da potência do computador e do nível de proteção desejado. A ativação de todos os recursos de verificação de vírus e spyware

pode alterar significativamente a velocidade do computador se você tiver um computador mais antigo.

25. Verificar se há malware

A verificação em tempo real protege o computador ao verificar todos os arquivos quando são acessados e ao bloquear o acesso aos arquivos que contêm *malware*.

A verificação em tempo real funciona da seguinte maneira:

a. Seu computador tenta acessar um arquivo.
b. O arquivo é imediatamente verificado em busca de *malware* antes que o computador tenha permissão para acessar o arquivo.
c. Se um *malware* for encontrado no arquivo, a verificação em tempo real remove o *malware* automaticamente, antes que ele possa danificar o computador.

26. A proteção em tempo real afeta o desempenho do computador?

Normalmente, o processo de verificação é imperceptível, pois é rápido e não utiliza muitos recursos do sistema. A quantidade de tempo e de recursos do sistema que a verificação em tempo real utiliza depende, por exemplo, do conteúdo, do local e do tipo de arquivo.

Arquivos cuja verificação é demorada:

- Os arquivos compactados, como os arquivos *.zip*.

Nota: Esses arquivos não são verificados por padrão.

- Arquivos em unidades removíveis como CDs, DVDs e unidades USB portáteis.

A verificação em tempo real pode tornar o computador mais lento se:

- você possui um computador bem antigo ou
- você acessa vários arquivos ao mesmo tempo. Um exemplo disso é abrir um diretório que contém vários arquivos com o Windows Explorer.

27. Ativar a verificação em tempo real

Ative a verificação em tempo real para impedir que um malware danifique o computador.

Para ativar a verificação em tempo real:

a. Na página principal, clique em Configurações.
b. Selecione Computador > Verificação de vírus e spyware.
c. Selecione Ativar verificação em tempo real.
d. Clique em OK.

28. Verificar se há malware no meu e-mail

A verificação de e-mail protege-o contra o recebimento ou o envio de vírus por e-mail.

A verificação de e-mail protege o computador contra:

- o recebimento de um vírus em um arquivo anexado a um e-mail que é enviado para você ou
- o envio acidental de um vírus para alguém, quando manda um e-mail com um arquivo anexado.

29. Quando as mensagens de e-mail e anexos são verificados

E-mails e seus anexos são verificados sempre que o programa envia ou recebe e-mails a partir do servidor de e-mail.

- As seguintes mensagens de e-mail são verificadas pela verificação de e-mail: As mensagens de e-mail enviadas e recebidas por programas de e-mail, como o Microsoft Outlook e o Outlook Express, o Microsoft Mail ou o Mozilla Thunderbird, que são executados como programas independentes do navegador da web.

As seguintes mensagens de e-mail não são verificadas pela verificação de e-mail:

- E-mails da web, os aplicativos de e-mail que são executados no navegador da web, como o Hotmail, Yahoo! mail ou Gmail.

Nota: Você precisa ter certeza de que as portas usadas para os diversos protocolos de e-mail (POP3, IMAP4, SMTP) estão corretamente configuradas. As mensagens de e-mail que são recebidas e enviadas através de outras portas não são verificadas.

Você ainda está protegido contra vírus, mesmo quando as portas não estão definidas corretamente ou quando você usa e-mail da web. Quando você abrir o anexo do e-

mail, a verificação em tempo real detectará se ele contém um vírus e bloqueará o vírus antes que ele possa causar danos.

Nota: A verificação em tempo real protegerá somente o seu computador,

30. Ativar e desativar a verificação do e-mail

Você pode ativar e desativar a verificação do e-mail como parte das configurações da verificação em tempo real.

Para ativar e desativar a verificação do e-mail:

a. Na página principal, clique em Configurações.
b. Selecione Computador > Verificação de vírus e spyware.
c. Escolha uma das seguintes ações:
   - Para ativar a verificação do e-mail, selecione Verificar e remover vírus dos e-mails.
   - Para desativar a verificação do e-mail, limpe Verificar e remover vírus dos e-mails.

Dependendo da sua escolha, a verificação do e-mail será ativada ou desativada.

31. Definir as portas usadas para diferentes protocolos de e-mails

Se o seu programa de e-mail usa uma porta que não seja padrão, você deve alterar a porta que é verificada para encontrar os vírus no e-mail. Caso contrário, essas mensagens de e-mail não passarão pela verificação de vírus.

Para definir as portas:

a. Abra seu programa de e-mail e verifique quais portas estão sendo usadas para enviar e receber e-mails. Anote os números das portas.
b. Abra o produto.
c. Na página principal, clique em Configurações.
d. Selecione Computador > Verificação de vírus e spyware.
e. Ao lado de Verificar e remover vírus dos e-mails, clique em Protocolos.
f. Insira o número da porta usada para cada um dos protocolos de e-mail, POP3, IMAP4 ou SMTP.

g. Clique em OK.

32. Ativar a verificação do tráfego da web

Você pode verificar a presença de vírus nas informações que passam pelo seu navegador para que o computador esteja protegido contra vírus enquanto navega na internet.

Para ativar a verificação do tráfego da web:

a. Na página principal, clique em Configurações.
b. Selecione Computador > Verificação de vírus e spyware.
c. Selecione Verificar e remover vírus do tráfego da web.
d. Clique em OK.
e. Se o navegador estava aberto quando você alterou a configuração, reinicie-o para que a alteração torne-se efetiva.

Quando você tenta fazer o download de um arquivo que possui um conteúdo suspeito ou malicioso, o download do arquivo ainda assim será feito, mas será preenchido com zeros em vez do conteúdo perigoso.

33. Bloquear cookies de rastreamento

Ao bloquear cookies de rastreamento, você evita que sites possam rastrear os sites que você acessa na Internet.

Os cookies de rastreamento são pequenos arquivos que permitem a websites registrarem os sites que você acessa. Para impedir que os cookies de rastreamento sejam instalados:

a. Na página principal, clique em Configurações.
b. Selecione Computador > Verificação de vírus e spyware.
c. Selecione Bloquear cookies de rastreamento.
d. Clique em OK.

34. Verificar em horários definidos

É possível verificar se há malware no computador em intervalos regulares, por exemplo diariamente, semanalmente ou mensalmente.

A verificação da presença de malware é um processo intenso. Ele requer a potência total de seu computador e leva algum tempo para ser concluído. Por esse motivo, defina o programa para verificar o computador quando ele não estiver em uso.

35. Agendar uma verificação

Você pode definir que o programa verifique o computador regularmente, por exemplo, semanalmente, diariamente ou mensalmente.

Para agendar uma verificação:

a. Na página principal, clique em Configurações.
b. Selecione Computador > Verificação programada.
c. Selecione Ativar verificação agendada.
d. Selecione os dias nos quais você deseja verificar, regularmente, a presença de vírus e spyware.

Opção	Descrição
Diariamente	Para verificar todos os dias.
Semanalmente	Para verificar em dias selecionados durante a semana. Selecione os dias de verificação na lista à direita.
Mensalmente	Para verificar até três dias por mês. Para selecionar os dias: ○ Selecione uma das datas. ○ Selecione o dia do mês na lista ao lado do dia selecionado. ○ Para verificar outro dia, repita.

e. Selecione quando você quer iniciar a verificação nos dias selecionados.

Opção	Descrição
Hora de início	A hora que será iniciada a verificação. Selecione um horário no qual você não espera usar o computador.
Depois que o computador não for usado por	Selecione um período de tempo após o qual o software deverá interpretar que você não está usando o computador e poderá iniciar a verificação.

36. Cancelar uma verificação agendada

Se desejar usar o computador quando uma verificação agendada for iniciada, é possível que você queira cancelar a verificação.

A verificação agendada pode ter um efeito notável no desempenho do computador. Para cancelar a verificação:

a. Clique no link A verificação agendada foi iniciada na notificação Verificação de vírus e spyware. A notificação permanece na tela por cerca de 15 segundos, e depois desaparece. Se você não clicar no link na notificação, você não poderá mais cancelar a verificação agendada.
b. Clique no link Cancelar na janela Verificação de vírus e spyware.
c. Clique no link Fechar.

A verificação agendada foi cancelada. A próxima verificação agendada irá acontecer normalmente.

37. Ver os resultados de verificação agendada

Quando uma verificação agendada for concluída, você pode verificar se algum malware foi encontrado.

Para verificar os resultados de uma verificação agendada:

a. Clique em A verificação agendada foi concluída na notificação Verificação de vírus e spyware.
b. Clique em Mostrar relatório para ver o que aconteceu durante a verificação.

Nota: Se você abriu a caixa de diálogo a partir da caixa de diálogo Histórico de notificações, o botão Exibir relatório está desativado. Não é possível ver os resultados das verificações agendadas anteriores.

c. Clique em Fechar para fechar a caixa de diálogo.

Dica: Você também pode ver os resultados da última verificação clicando em Configurações > Computador > Verificação agendada. Clique em Ver último relatório de verificação.

38. Verificar manualmente

Verifique o computador manualmente se suspeitar a existência de malware no computador.

39. Como selecionar o tipo de verificação manual

É possível verificar todo o computador, um tipo específico de malware ou um local específico.

Se você suspeitar que há um determinado tipo de malware, poderá verificar somente esse tipo. Se você suspeitar de um determinado local em seu computador, poderá verificar somente aquela seção. Essas verificações serão concluídas de forma mais rápida do que uma verificação de todo o computador.

Para iniciar a verificação manual em seu computador:

a. Na página principal, clique na seta logo abaixo de Verificar. As opções de verificação são mostradas.
b. Selecione o tipo de verificação. Se desejar alterar as configurações de verificação, selecione Alterar configurações de verificação.
c. Se você selecionou Escolher o que verificar, uma janela será aberta na qual é possível selecionar qual local verificar.

O Assistente de Verificação será aberto.

40. Tipos de verificação

É possível verificar todo o computador, um tipo específico de malware ou um local específico.

A lista a seguir mostra os diferentes tipos de verificação:

Tipo de verificação	O que é verificado	Quando utilizar este tipo
Verificação completa do computador	Todo o computador (discos rígidos internos e externos) em busca de vírus, spyware e *riskware*	Para ter certeza absoluta de que não há malware ou *riskware* em seu computador. Este tipo de verificação demora mais tempo para ser concluída. Ela combina a verificação rápida de malware e a verificação de disco rígido. Ela também verifica os itens que possivelmente estão ocultos por rootkit.

Escolher o que verificar...	Um arquivo ou pasta específica em busca de vírus, spyware e *riskware*	Se você suspeitar que há malware em um local específico de seu computador, por exemplo, o local contém downloads de fontes potencialmente perigosas, como redes ponto a ponto de compartilhamento de arquivos. A duração da verificação dependerá do tamanho do destino que você verificar. A verificação termina mais rapidamente se, por exemplo, uma pasta que contém somente poucos arquivos pequenos for verificada.
Verificar discos rígidos	Todos os discos rígidos internos no seu computador em busca de vírus, spyware e *riskware*	Este tipo de verificação passa por todos os discos rígidos do computador. Diferente da verificação rápida de malware, este tipo de verificação não passa especificamente pelas partes do seu sistema que contenham programas instalados, mas também verifica todos os arquivos de dados, como documentos, músicas, imagens e vídeos. Este tipo de verificação é lento e é recomendado apenas se a verificação rápida de malware não encontrou nenhum malware e se você desejar ter certeza de que todas as outras partes do computador não contêm arquivos maliciosos.
Verificação de vírus e spyware	Partes do computador em busca de vírus, spyware e *riskware*	Este tipo de verificação é muito mais rápida que uma verificação completa. Ela pesquisa apenas as partes do sistema que contenham arquivos de programas instalados. Esse tipo de verificação é recomendado se você desejar verificar rapidamente se o computador está limpo, porque ele pode encontrar e remover com eficiência qualquer malware ativo no computador.
Verificação de *rootkit*	Locais importantes do sistema onde um item suspeito pode significar um problema de segurança. Verifica se há arquivos, pastas, unidades ou processos ocultos	Quando você suspeitar que um *rootkit* pode estar instalado no computador. Por exemplo, se um malware foi recém-detectado no computador e você deseja certificar-se de que ele não instalou um rootkit.

41. Limpar malware automaticamente

Se malware for encontrado durante a verificação, você pode deixar o programa decidir automaticamente como limpar seu computador ou pode decidir você mesmo o que fazer com cada item.

a. Selecione uma das seguintes opções:

Opção	O que acontecerá
Resolver automaticamente (recomendado)	O programa decide o que fazer com cada item de *malware* para limpar automaticamente o computador.
Desejo decidir item por item	O programa pergunta o que você deseja fazer com cada *malware*.

b. Clique em Avançar.

42. Ver os resultados da verificação manual

Após a conclusão da verificação, você pode ver um relatório dos resultados da verificação.

Nota: É possível que você queira ver esse relatório já que a ação selecionada por você talvez não seja sempre realizada. Por exemplo, se você escolher limpar um arquivo infectado, mas o vírus não pôde ser removido do arquivo, o produto talvez tenha realizado outra ação com o arquivo.

Para ver o relatório:

a. Clique em Mostrar Relatório. O relatório inclui:
   - A quantidade de malware encontrada.
   - O tipo de malware encontrado e links para as descrições do malware na internet.
   - As ações aplicadas a cada malware.
   - Quaisquer itens que tenham sido excluídos da verificação.
   - Os mecanismos de verificação que foram usados para verificar malware.

Nota: O número de arquivos verificados pode variar se arquivos dentro de arquivos compactados forem verificados. Se arquivos compactados foram verificados anteriormente, os resultados da verificação podem estar salvas na memória cache.

Clique em Finalizar para fechar o Assistente de Verificação.

Dica: Você também pode visualizar os resultados da última verificação clicando em Configurações > Computador > Verificação manual. Clique em Visualizar último relatório de verificação.

43. Selecionar arquivos que serão verificados

Selecione os tipos de arquivos e partes do computador a serem verificados nas verificações manuais e agendadas.

Nota: Edite as configurações de verificação manual para selecionar arquivos e pastas que deseja verificar durante a verificação agendada.

Dois tipos de lista determinam quais arquivos são verificados em tempo real em busca de vírus:

- Uma lista de tipos de arquivos que contém todos os arquivos ou uma lista definida de tipos de arquivos.
- Listas de arquivos excluídos da verificação definem exceções da lista de arquivos verificados. Os tipos de arquivos ou os locais nessas listas de exclusão não serão verificados, mesmo que eles estejam presentes na lista de "inclusão".

As listas de "inclusão" e "exclusão" permitem definir que partes do computador serão verificadas e de que maneiras:

- É possível incluir todos os arquivos e depois, opcionalmente, usar a lista de exclusão para excluir as unidades, diretórios ou arquivos que você sabe que são seguros e não deseja verificar.
- Você pode definir uma lista de tipos de arquivos que deseja verificar para que somente esses arquivos sejam verificados.

44. Incluir arquivos

Você pode selecionar os tipos de arquivo que você deseja verificar em busca de vírus e spyware em verificações manuais ou agendadas.

a. Na página principal, clique em Configurações.
b. Selecione Computador > Verificação manual.

c. Em Opções de verificação, selecione o seguinte:

Verificar apenas os tipos de arquivo conhecidos (mais rápido)	Para verificar apenas aqueles tipos de arquivos que têm mais probabilidade de conter infecções como, por exemplo, arquivos executáveis. Selecionar esta opção também torna a verificação mais rápida.
Verificar arquivos compactados (.zip, .rar, etc.)	Para verificar pastas e arquivos compactados.
Usar heurística avançada (mais lento)	Para usar todas as heurísticas durante a verificação para encontrar melhor malware novos ou desconhecidos. **Nota:** Se selecionar essa opção, a verificação levará mais tempo e podem ocorrer mais falsos positivos (arquivos inofensivos reportados como suspeitos).

d. Clique em OK.

As opções que você selecionar em Opções de verificação determina quais arquivos são inclusos em verificações manuais e agendadas futuras.

Nota: Todos os tipos de arquivos ou locais na lista de itens excluídos substituirão as configurações definidas aqui. Tipos de arquivos na lista de itens excluídos não serão verificados mesmo se você selecioná-los para ser verificados aqui.

45. Excluir tipos de arquivo

Você pode excluir arquivos das verificações manuais e em tempo real segundo o tipo do arquivo.

a. Na página principal, clique em Configurações.

b. Proceda de uma das seguintes maneiras:

- Selecione Computador > Verificação de vírus e spyware.
- Selecione Computador > Verificação manual.

c. Clique em Abrir lista de itens excluídos.

d. Para excluir um tipo de arquivo:

- Selecione a guia Tipos de Arquivo.
- Selecione Excluir arquivos com estas extensões.

- Digite uma extensão de arquivo que identifique o tipo de arquivo que você deseja excluir no campo próximo ao botão Adicionar. Para especificar arquivos que não têm extensão, digite '.'. Você pode usar o coringa '?' para representar qualquer caractere único ou '*' para representar qualquer número de caracteres. Por exemplo, para excluir arquivos executáveis, digite exe no campo.
- Clique em Adicionar.

e. Repita a etapa anterior para excluir qualquer outra extensão da verificação de vírus.
f. Clique em OK para fechar a caixa de diálogo Excluir da Verificação.
g. Clique em OK para aplicar as novas configurações.

Os tipos de arquivo selecionados são excluídos das verificações manuais e em tempo real futuras.

46. Excluir arquivos de acordo com o local

Você pode definir uma lista de pastas ou unidades excluídos que não queira que sejam verificados em busca de vírus em verificações manuais ou em tempo real.

Nota: Arquivos em pastas ou unidades excluídos da verificação não são verificados, mesmo que sejam de um tipo incluído nos tipos de arquivos verificados.

Para definir uma lista de arquivos, pastas ou unidades excluídos de acordo com o local:

a. Na página principal, clique em Configurações.
b. Proceda de uma das seguintes maneiras:
   - Selecione Computador > Verificação de vírus e spyware.
   - Selecione Computador > Verificação manual.
c. Clique em Abrir lista de itens excluídos.
d. Para excluir um arquivo, unidade ou pasta:
   - Selecione a guia Objetos.
   - Selecione Excluir objetos (arquivos, pastas, ...).
   - Clique em Adicionar.
   - Selecione o arquivo, unidade ou pasta a ser excluído da verificação em busca de vírus.

Nota: Algumas unidades podem ser removíveis, como CD, DVD, ou unidades de rede. Unidades de rede e unidades removíveis vazias não podem ser excluídas.

- Clique em OK.

e. Repita a etapa anterior para excluir outros arquivos, unidades ou pastas da verificação contra vírus.
f. Clique em OK para fechar a caixa de diálogo Excluir da Verificação.
g. Clique em OK para aplicar as novas configurações.

Os arquivos, unidades ou pastas selecionados serão excluídos de verificações manuais e em tempo real futuras.

47. Ver aplicativos excluídos

Você pode ver aplicativos que excluiu de verificações em tempo real, manuais e agendadas futuras, e removê-los da lista de excluídos para que sejam encontrados em verificações futuras.

Para ver os aplicativos que foram excluídos da verificação:

a. Na página principal, clique em Configurações.
b. Proceda de uma das seguintes maneiras:
   - Selecione Computador > Verificação de vírus e spyware.
   - Selecione Computador > Verificação manual.
c. Clique em Abrir lista de itens excluídos.
d. Selecione a guia Aplicativos.

Nota: Apenas aplicativos de spyware e riskware podem ser excluídos, não vírus.

e. Para restaurar um aplicativo para que ele seja localizado em futuras verificações manuais ou agendadas:
   - Selecione o aplicativo que deseja incluir na verificação novamente.
   - Clique em Remover.
f. Clique em OK para fechar a caixa de diálogo Excluir da Verificação.
g. Clique em OK para sair.

48. Verificar dentro de arquivos e pastas compactadas

Você pode verificar por vírus em arquivos e pastas compactados.

a. Na página principal, clique em Configurações.
b. Selecione Computador > Verificação manual.
c. Para verificar arquivos e pastas compactados, como os arquivos .zip, selecione Verificar arquivos compactados (.zip, .rar, etc.). A verificação de arquivos compactados demora um pouco mais.
d. Clique em OK.

49. Selecionar a ação quando algo for encontrado

Se vírus forem encontrados e você não definiu o programa para processar vírus automaticamente, você pode selecionar agora se quer limpá-los, excluí-los, colocá-los em quarentena ou apenas bloquear os arquivos nos quais os vírus foram encontrados.

Nota: Essa etapa do Assistente de Verificação será ignorada se você tiver definido o programa para sempre lidar com o vírus automaticamente durante a verificação manual ou agendada ou se tiver definido o programa para processar automaticamente o malware encontrado durante essa verificação.

Será exibida uma lista de arquivos infectados e dos vírus encontrados nestes arquivos. Para lidar com estes vírus do computador:

a. Selecione a ação a ser tomada para arquivos infectados. Se desejar visualizar os detalhes adicionais da infecção, clique no link na coluna Infecção.
b. Clique em Avançar para aplicar as ações.
c. Clique em Avançar para concluir.

Se o spyware for encontrado durante a verificação manual ou agendada, o Assistente de verificação continua a etapa de limpeza de spyware.

50. Ações a realizar em caso de arquivos infectados

A coluna Ação a ser realizada mostra que ações você pode realizar em caso de arquivos infectados na verificação em tempo real, manual ou agendada.

As seguintes ações podem ser realizadas em caso de arquivos infectados:

Nota: Além de atingir arquivos, a infecção também pode ser encontrada em uma entrada de registro ou em um processo.

Ação a ser realizada	O que acontece com os arquivos infectados
Limpar os arquivos	Se possível, o *vírus* é removido dos arquivos infectados. Após isso, é seguro utilizar os arquivos
Excluir os arquivos	Os arquivos infectados são excluídos
Colocar os arquivos em quarentena	Os arquivos infectados são movidos para a quarentena, onde não poderão danificar o computador. Posteriormente, você poderá liberar o arquivo da quarentena, se necessário.
Apenas bloquear o arquivo	O acesso ao arquivo infectado é bloqueado.

51. Ações padrão na verificação em tempo real

A coluna Ação padrão mostra quais ações padrão é possível selecionar para arquivos infectados na verificação em tempo real.

É possível selecionar uma das seguintes ações padrão se um malware for encontrado:

Ação padrão	O que acontece se um malware for encontrado
Perguntar sempre	O programa pergunta o que fazer se o malware for encontrado durante uma verificação em tempo real.
Perguntar quando não estiver claro	Quando o programa não puder identificar o malware, ele pergunta o que você deseja fazer com ele.

52. Ações padrão na verificação manual e agendada

A coluna Ação padrão mostra quais ações padrão é possível selecionar para arquivos infectados na verificação manual e agendada.

É possível selecionar uma das seguintes ações padrão se um malware for encontrado:

Ação padrão	O que acontece se um malware for encontrado
Perguntar	O programa pergunta o que fazer se o malware for encontrado

sempre	durante uma verificação manual. **Nota:** Em verificações agendadas, essa opção executa a mesma ação que a opção Limpar os arquivos.
Limpar os arquivos	O programa tenta limpar os vírus automaticamente em qualquer arquivo infectado que for encontrado durante uma verificação manual ou agendada. Spyware e *riskware* são automaticamente colocados em quarentena. **Nota:** Nem sempre é possível limpar um vírus em um arquivo. Se isso não for possível, o arquivo é colocado em quarentena (exceto quando encontrado em unidades de rede ou removíveis), portanto o vírus não pode danificar o computador.
Excluir os arquivos	O programa automaticamente exclui qualquer arquivo infectado encontrado durante uma verificação manual ou agendada.
Colocar os arquivos em quarentena	O programa automaticamente move qualquer arquivo infectado encontrado durante uma verificação manual ou agendada para a quarentena, onde ele não poderá danificar o computador.
Somente relatório	O programa deixa qualquer arquivo infectado encontrado durante uma verificação manual ou agendada como está e registra a detecção do malware no relatório de verificação. **Nota:** Se a proteção em tempo real não estiver ativada, qualquer malware ainda poderá danificar o computador se você selecionar essa opção.

53. Ações padrão para o DeepGuard

A coluna Ação padrão mostra quais ações padrão é possível selecionar para o DeepGuard.

É possível selecionar uma das seguintes ações padrão se o DeepGuard detectar uma tentativa de modificação do sistema:

Ação padrão	O que acontece se um malware for encontrado
Perguntar sempre	O DeepGuard pergunta se você deseja permitir ou bloquear todas as ações monitoradas, mesmo quando ele identifica que o aplicativo é seguro.
Perguntar quando não estiver claro	O DeepGuard pergunta se você deseja permitir ou bloquear ações monitoradas apenas quando ele não puder identificar o aplicativo como seguro ou não seguro
Resolver automaticamente	O DeepGuard bloqueia os aplicativos não seguros e permite os aplicativos seguros automaticamente, sem fazer nenhuma pergunta.

54. Ver histórico de vírus e spyware

O histórico de vírus e spyware mostra o que o programa fez com os vírus e *spywares* encontrados.

Para ver o histórico:

a. Na página principal, clique em Configurações.

b. Selecione Computador > Verificação de vírus e spyware.

c. Clique em Ver histórico de vírus e spyware.

O histórico de vírus e spyware é aberto.

55. O que é o DeepGuard?

O DeepGuard analisa o conteúdo de arquivos e o comportamento de programas e bloqueia vírus, worms e outros programas maliciosos novos e ainda não descobertos que tentam fazer alterações potencialmente perigosas no computador.

As alterações do sistema que podem ser perigosas incluem:

- alterações na configuração do sistema (Registro do Windows),
- tentativas de desativar programas de sistema importantes, por exemplo, os programas de segurança como este produto e
- tentativas de editar os arquivos de sistema importantes.

O DeepGuard observa continuamente essas alterações e verifica cada programa que tentar alterar o sistema.

56. Como o DeepGuard funciona

Quando o DeepGuard detecta um programa tentando fazer alterações potencialmente perigosas no sistema, ele permitirá que o programa seja executado em uma zona segura, a menos que você tenha dado permissão ao programa ou que o tenha bloqueado de maneira específica.

Na zona segura, o programa não consegue danificar o computador. O DeepGuard analisa que alterações o programa tentou fazer e, com base nisso, decide qual é a probabilidade de o programa ser um malware.

O DeepGuard permite ou bloqueia o programa automaticamente, ou pergunta se deve permitir ou bloquear o programa, dependendo:

- da probabilidade de o programa ser ou não um malware e
- de que ação o DeepGuard foi solicitado a realizar quando ele detectar uma tentativa potencialmente perigosa de alterar o sistema.

57. Como ativar o DeepGuard

Ao ativar o DeepGuard, você pode evitar que programas suspeitos façam alterações potencialmente perigosas no sistema do computador.

Antes de ativar o DeepGuard, certifique-se de que você tenha o Service Pack 2 instalado e de que tenha o Windows XP.

Para ativar o DeepGuard:

a. Na página principal, clique em Configurações.
b. Selecione Computador > DeepGuard.
c. Selecione Ativar DeepGuard.
d. Clique em OK.

58. Permitir programas que o DeepGuard bloqueou

Você pode permitir que um programa que o DeepGuard tenha bloqueado faça alterações no sistema.

Às vezes o DeepGuard pode evitar que um programa seguro seja executado, mesmo se você quiser usar o programa e souber que é seguro. Isso acontece porque o programa tenta fazer alterações no sistema que podem ser potencialmente perigosas. Você também pode ter bloqueado um programa sem intenção quando uma janela pop-up do DeepGuard foi mostrada. É possível liberar um programa bloqueado alterando sua permissão na lista Programas.

Para permitir um programa que o DeepGuard bloqueou:

a. Na página principal, clique em Tarefas.
b. Clique em Permitir que um programa seja iniciado. A lista dos programas é exibida.
c. Clique na coluna Permissão para organizar a lista em grupos de programas permitidos e negados.
d. Selecione o programa que você deseja permitir e clique em Detalhes.
e. Em Permissão, selecione Permitir.
f. Clique em OK.

g. Clique em Fechar.

O programa que você selecionou agora está permitido para ser executado e fazer alterações no sistema.

59. Como desativar o monitoramento avançado de processos

Para obter a máxima proteção, o DeepGuard modifica temporariamente programas em execução.

Alguns programas, como jogos on-line e ferramentas antitrapaça, podem falhar por causa desse monitoramento avançado de processos. Isso acontece com programas que verificam sua própria integridade. Geralmente ferramentas antitrapaça usam a verificação de integridade para descobrir se foram modificadas para fazer outra coisa além daquilo para o qual foram criadas.

Para desativar o monitoramento avançado de processos:

a. Na página principal, clique em Configurações.

b. Selecione Computador > DeepGuard.

c. Desmarque Usar monitoramento de processo avançado.

d. Clique em OK.

60. Proteger contra alterações perigosas no sistema

Se o DeepGuard detectar um programa tentando fazer alterações potencialmente perigosas no sistema e não puder identificar se o programa é seguro ou não, ele exibe uma caixa de diálogo Tentativa de modificação do sistema.

A caixa de diálogo Tentativa de modificação do sistema é mostrada se você selecionou uma das seguintes opções como a ação a ser tomada pelo DeepGuard quando detectar uma tentativa potencialmente perigosa de alterar o sistema:

- Perguntar sempre ou
- Perguntar quando não estiver claro.

O DeepGuard pode mostrar a caixa de diálogo, por exemplo, quando você estiver instalando algum software.

Para decidir se o programa que está tentando fazer as alterações no sistema é confiável:

a. Se você não tiver certeza da origem da tentativa de modificação, clique em Detalhes >> para ver mais informações sobre o programa. A seção Detalhes técnicos mostra:
   - o nome do programa que está tentando fazer a alteração,
   - a localização do programa,
   - a alteração que o programa está tentando fazer e
   - a pontuação de risco, que indica a probabilidade de o programa ser um malware:
     1. uma pontuação baixa indica um programa que provavelmente não representa nenhum perigo e
     2. uma pontuação alta indica um programa que provavelmente é um malware.

b. Selecione uma das seguintes opções:

Selecione...	Se...
Eu confio no aplicativo. Deixe-o continuar.	Acha que o programa é seguro. A probabilidade de o programa ser seguro é maior se: tiver uma baixa *pontuação de risco*, a caixa de diálogo for exibida como consequência de alguma ação de sua parte, você reconhecer o programa ou você tiver obtido o programa de uma fonte segura.
Eu não confio no aplicativo. Bloquear a operação.	Suspeita que o programa não é seguro. A probabilidade de o programa não ser seguro é maior se: tiver uma alta *pontuação de risco*, você não conhecer o programa ou você conhecer o programa e acreditar que ele é suspeito.

c. Selecione Não mostrar esta caixa de diálogo para este programa novamente se você desejar que o DeepGuard aplique suas decisões para esse programa quando ele tentar fazer alterações no sistema no futuro. Essa opção estará visível somente se você selecionou Sempre perguntar como a ação em caso de tentativas de modificação do sistema. Na próxima vez que o DeepGuard detectar o mesmo programa, ele não perguntará a você o que fazer, mas aplicará sua decisão anterior.

d. Para enviar uma amostra de um programa que tentou executar alterações no sistema, proceda da seguinte maneira:
   - Clique em Enviar uma amostra... Uma caixa de diálogo que explica as condições do envio é exibida.

- Leia cuidadosamente as condições e clique em Aceito se você concordar com as condições e desejar enviar a amostra.

Você talvez deva enviar uma amostra:

- se o DeepGuard bloquear automaticamente um programa que você sabe que é seguro ou
- quando uma caixa de diálogo Tentativa de modificação do sistema for exibida e você suspeitar que o programa seja um malware.

O sistema envia ao Oi uma cópia eletrônica do programa, que foi identificado como uma possível ameaça à segurança.

61. Como ver o que o DeepGuard fez

Uma pequena notificação é exibida quando o DeepGuard impede automaticamente um programa de fazer alterações no sistema.

Notificações são pequenos lembretes exibidos no canto inferior direito da tela do computador. Eles são exibidos, por exemplo, se o DeepGuard negar o uso de um programa. Essas notificações são informacionais e não requerem nenhuma ação sua. Você pode ver todas as notificações exibidas no histórico de notificações.

Se um programa que você tentar instalar ou executar não funcionar, pode ser porque o DeepGuard está impedindo o programa de fazer alterações no sistema. Neste caso, você pode fazer com que o DeepGuard exiba uma pequena notificação quando bloquear um programa automaticamente. Assim, você sabe porque o programa não funcionou corretamente.

62. Como utilizar a quarentena

A quarentena é um repositório seguro para arquivos que podem ser perigosos.

Os arquivos em quarentena não conseguem disseminar ou causar qualquer dano ao seu computador.

Você pode colocar o malware, spyware e *riskware* em quarentena para impedir que eles causem danos. Se necessário, também é possível restaurar aplicativos ou arquivos da quarentena posteriormente.

Se você não precisar de um item em quarentena, pode exclui-lo. A exclusão de um item da quarentena remove-o permanentemente do computador.

- Em geral, é possível excluir um malware que está em quarentena.
- Na maioria das vezes, você pode excluir o spyware que está em quarentena. É possível que o spyware em quarentena faça parte de um programa legítimo e a sua remoção poderá impedir o programa de funcionar corretamente. Para manter o programa no computador, você pode restaurar o spyware que está em quarentena.
- Um riskware que está em quarentena pode ser um programa legítimo. Se você mesmo instalou e configurou o programa, poderá restaurá-lo da quarentena. Se o riskware foi instalado sem o seu conhecimento, é muito provável que tenha sido instalado com intenções maliciosas e deverá ser excluído.

63. Ver itens em quarentena

Você pode ver mais informações sobre os itens em quarentena.

Para ver informações detalhadas sobre os itens em quarentena:

a. Na página principal, clique em Tarefas.
b. Na página Tarefas, clique em Restaurar um arquivo ou programa removido. A caixa de diálogo Quarentena é aberta.
c. Navegue pelas categorias Vírus, Spyware e Riskware para ver todos os itens em quarentena.
   - A lista de vírus em quarentena exibe o nome do item em quarentena e o caminho onde o arquivo estava instalado. Se o item em quarentena instalou vários arquivos, a lista o exibirá como infecção do sistema.
   - A lista de spyware em quarentena exibe o tipo de spyware e uma lista de aplicativos conhecidos por ter spyware anexados.
   - A lista de riskware em quarentena exibe o caminho e o nome de arquivo do item em quarentena.
d. Para ver mais informações sobre o item em quarentena, selecione uma das seguintes opções:
   - Clique no ícone próximo ao item em quarentena.
   - Clique em Detalhes para ver mais informações sobre o item em quarentena.
e. Para excluir o item em quarentena, selecione o item e clique em Excluir.

64. Restaurar itens da quarentena

É possível restaurar os itens da quarentena, se for necessário.

É possível restaurar aplicativos ou arquivos da quarentena se for necessário. Não restaure itens da quarentena a menos que você tenha certeza de que não podem causar danos. Os itens restaurados são colocados de volta no local original no seu computador.

a. Na página principal, clique em Tarefas.
b. Na página Tarefas, clique em Restaurar um arquivo ou programa removido. A caixa de diálogo Quarentena é aberta.
c. Navegue pelas categorias de quarentena e selecione o item a ser restaurado. É possível selecionar vários itens para restauração.

Nota: Ao selecionar arquivos, observe que o nome do item na quarentena funciona como um link para a descrição do item no banco de dados on-line.

d. Clique em Restaurar. O produto restaura o item selecionado de volta para o local original na unidade de disco e remove o item da lista da quarentena.

65. Como utilizar as atualizações automáticas

A opção atualizações automáticas mantém a proteção no computador atualizada.

O produto salva as atualizações mais recentes no computador quando você está conectado à internet. Ele detecta o tráfego da rede e não interrompe o uso da internet mesmo que a conexão da rede seja lenta.

66. Verificar o status da atualização

Visualizar a data e a hora da última atualização.

Quando as atualizações automáticas estão ativadas, o produto recebe as últimas atualizações quando você estiver conectado à internet.

Para verificar se as atualizações são as mais recentes:

a. Na página principal, clique em Configurações.
b. Selecione Outras configurações > Atualizações automáticas.

c. Clique em Verificar agora. O produto conecta-se à internet e verifica as últimas atualizações. Se a proteção não estiver atualizada, ele recuperará as últimas atualizações.

Nota: Se você estiver usando um modem ou tiver uma conexão ISDN com a internet, a conexão deverá estar ativa para verificar a presença de atualizações.

67. Alterar minhas configurações de conexão à internet

É possível configurar a maneira como o computador conecta-se à internet para que você possa receber atualizações automaticamente.

Para alterar as configurações de conexão à internet:

Nota: Em geral, não é necessário alterar as configurações padrão.

a. Na página principal, clique em Configurações.
b. Selecione Outras configurações > Conexão.
c. Na lista Conexão à internet, selecione como o seu computador está conectado à internet.
   - Selecione Supor que está sempre conectado se houver uma conexão de rede permanente.

Nota: Se, na realidade, o seu computador não tiver uma conexão de rede permanente e estiver configurado para discagem sob demanda, a seleção de Supor que está sempre conectado poderá resultar em várias discagens.

   - Selecione Detectar conexão para recuperar atualizações somente quando o produto detectar uma conexão de rede ativa.
   - Selecione Detectar tráfego para recuperar atualizações somente quando o produto detectar outro tráfego de rede.

Dica: Se houver uma configuração de hardware incomum que faça a configuração Detectar conexão detectar uma conexão de rede ativa mesmo quando ela não existe, opte pela seleção de Detectar tráfego.

d. Na lista Proxy HTTP, selecione se deseja ou não que o computador use um servidor proxy para se conectar à internet.
   - Selecione Nenhum Proxy HTTP se o seu computador estiver conectado diretamente à internet.
   - Selecione Configurar proxy HTTP manualmente para definir as configurações do Proxy HTTP.
   - Selecione Usar o proxy HTTP de meu navegador para usar as mesmas configurações do Proxy HTTP que você definiu no seu navegador da web.

68. Verificar o status da Rede de proteção em tempo real

Para funcionar adequadamente, muitos recursos do produto dependem da conectividade com a rede de Proteção em tempo real.

Se houver problemas de rede ou se o firewall bloquear o tráfego da Rede de proteção em tempo real, o status será "desconectada". Se nenhum dos recursos instalado necessitarem do acesso à Rede de proteção em tempo real, o status é "sem uso".

Para verificar o status:

a. Na página principal, clique em Configurações.

b. Selecione Outras configurações > Conexão.

Em Rede de proteção em tempo real, você pode ver o status atual da Rede de proteção em tempo real.

69. Ativar as atualizações automáticas

Quando você mantém as atualizações automáticas ativadas, o produto se mantém atualizado automaticamente.

a. Na página principal, clique em Configurações.

b. Selecione Outras configurações > Atualizações automáticas.

c. Selecione Ativar atualizações automáticas.

70. Segurança das conexões de rede

O software protege o computador contra tráfego de internet inseguro.

- Protege contra os invasores que tentam acessar o computador sem a sua permissão. Eles podem, por exemplo, tentar roubar informações pessoais, como arquivos, senhas ou números de cartões de crédito.
- Bloqueia o tráfego malicioso da internet, como os Cavalos de Tróia. Eles podem, por exemplo, destruir arquivos em seu computador, travar o computador ou abrir portas para que hackers acessem o computador.
- Bloqueia o tráfego perigoso da internet, como os spywares. Os spywares podem, por exemplo, coletar informações sobre os seus endereços de e-mail, senhas e números de cartões de crédito.
- Impede que os programas de discador maliciosos usem o seu modem ou conexão ISDN para discar números de telefone caros que são pagos por minuto.

Depois de ter instalado o software, suas conexões de rede são automaticamente protegidas.

71. O que é um firewall

O firewall protege o computador permitindo o tráfego seguro e bloqueando o tráfego não seguro da internet.

Geralmente, o firewall permite todo o tráfego do computador para a internet, mas bloqueia todo o tráfego da internet para o computador, a menos que você especificamente o permita. Ao bloquear o tráfego de entrada, o firewall protege o computador contra os softwares maliciosos, como os worms, e impede que invasores acessem o computador. Dependendo das configurações dos alertas, as pop-ups dos alertas do firewall talvez sejam mostradas sobre as ações do firewall.

O seu computador é protegido por configurações de firewall predefinidas. Geralmente, não é necessário alterá-las. Entretanto, talvez seja necessário alterar as configurações, se você usar um perfil de firewall muito estrito, ou se você adicionou suas próprias regras de firewall ou serviços.

CUIDADO: Não desative o firewall. Se fizer isso, o computador ficará vulnerável a todos os ataques através da rede. Se, por exemplo, um programa parar de funcionar no

computador porque não consegue acessar a internet, altere as configurações das regras de firewall ou do controle de aplicativos em vez de desativar o firewall

72. O que são perfis de firewall

O *perfil de firewall* define o nível de proteção no computador.

Cada *perfil de firewall* tem um conjunto predefinido de *regras de firewall,* que define o tipo de tráfego permitido ou negado no computador. Para alguns perfis você também pode adicionar regras que você mesmo criou.

Perfis de firewall também definem

- se conexões com a internet são permitidas automaticamente para todos os aplicativos ou
- se você pode permitir ou negar separadamente cada nova tentativa de conexão em uma janela pop-up do controle de aplicativos.

Estes são vários *perfis de firewall* predefinidos, que vão de muito estritos a muito livres:

- Um perfil de firewall muito estrito (Bloquear tudo) geralmente bloqueia a maioria do tráfego da rede. Isso pode impedir que você use alguns dos programas do computador.
- Um perfil médio (Normal) geralmente permite todo o tráfego de saída da internet do computador. O perfil médio pode negar alguns serviços de entrada e gerar alertas sobre eles.
- Um perfil muito livre (Permitir tudo) geralmente permite todo o tráfego da rede, tanto de entrada como de saída, e não gera alertas. Pelo fato deste perfil deixar seu computador desprotegido, não use-o exceto em casos especiais.

Nota: Dependendo do produto que estiver usando, os nomes dos perfis de firewall podem ser diferentes.

Seu computador estará seguro com o *perfil de firewall* predefinido. Talvez seja necessário alterar o nível para um mais rígido, por exemplo, se você usar o laptop fora de casa e abrir a internet usando uma conexão *WLAN*.

Você pode definir seus próprios *perfis de firewall* e adicionar seu próprio conjunto de regras a ele. Entretanto, recomendamos que apenas usuários experientes definam seus próprios perfis de firewall.

73. Como os perfis de firewall estão relacionados a serviços e regras

Um *perfil de firewall* consiste em várias *regras de firewall*. Uma *regra de firewall* consiste de vários *serviços de firewall*. Serviços são definidos pelos *protocolos* e *portas* que usam.

Por exemplo, o perfil de firewall Móvel tem uma regra chamada Navegação na web. Essa regra permite que você navegue na web. A regra inclui os serviços que são necessários para a navegação na web, como o serviço HyperText Transfer Protocol (HTTP). Esse serviço usa o TCP *e a porta* de número 80.

74. Como alterar o perfil de firewall

Se você desejar alterar o nível de proteção no seu computador, altere o perfil de firewall.

Para alterar o perfil de firewall:

a. Na página principal, clique em Status.
b. Ao lado de Firewall, clique no link, que mostra o perfil de firewall atual. A caixa de diálogo Perfil de firewall para conexões de rede é aberta.
c. Leia cuidadosamente as descrições do perfil de firewall.
d. Selecione o perfil adequado na lista e clique em OK.

A página Status agora mostra o novo perfil de firewall. As regras de firewall e configurações do controle de aplicativos variam de acordo com o perfil de firewall selecionado.

75. O que são serviços e regras de firewall

Serviços e regras de firewall definem como o firewall protege suas conexões de rede.

76. O que são regras de firewall

As *regras de firewall* definem que tipo de tráfego da internet é permitido ou bloqueado.

Cada *perfil de firewall* tem um conjunto predefinido de *regras de firewall*, que você não pode alterar. Você pode apenas adicionar novas regras para alguns dos perfis. Para alguns perfis você talvez não possa adicionar suas próprias regras. Também pode haver um perfil que não tenha regras predefinidas e que permita que você adicione livremente seu próprio conjunto de regras. O perfil de firewall selecionado também afeta a prioridade que suas próprias regras recebem em relação às regras predefinidas.

Uma *regra de firewall* pode ser aplicada ao tráfego da internet para o computador (entrada) ou do computador para a internet (saída). Uma regra pode ser aplicada nas duas direções ao mesmo tempo.

Uma *regra de firewall* é formada de *serviços de firewall*, que especificam o tipo de tráfego e as *portas* que esse tipo de tráfego usa. Por exemplo, uma regra nomeada Navegação na web possui um serviço nomeado HTTP, que usa TCP e a *porta* de número 80.

As *regras de firewall* também definem se janelas pop-up de *alertas* do firewall são mostradas para você sobre o tráfego que corresponde às *regras de firewall*.

77. Quando é necessário adicionar uma nova regra de firewall?

Pode ser necessário adicionar uma nova regra de firewall se você for usar um novo programa ou anexar um novo dispositivo ao computador, por exemplo, um dispositivo WLAN ou uma câmera IP.

Ao adicionar todos os serviços que o programa ou dispositivo necessita para a mesma regra, você pode facilmente:

- ativar ou desativar a regra mais tarde ou
- remover a regra se você desinstalar o programa ou remover o dispositivo.

Você também precisa adicionar uma nova regra se negou algum tipo de tráfego mas desejar permiti-lo para alguns endereços IP. Neste caso, você já tem uma *regra de firewall* de "negação" geral. Para permitir o tráfego para determinados endereços IP, você deverá criar uma regra de "permissão" mais específica.

Por exemplo, se a regra geral negar todo o tráfego de saída do *FTP*, talvez você ainda queira permitir o tráfego do *FTP* para o site do seu provedor de serviços da internet e assim poder atualizar as páginas da web. Isso será possível se você adicionar uma regra mais específica que permita o tráfego do *FTP* para o endereço IP do provedor de serviços da internet, e dar a essa regra uma prioridade mais alta do que à regra de "negação".

78. Ver regras de firewall

É possível exibir as regras de firewall ativas no momento para saber como o firewall permite ou bloqueia o tráfego do computador.

Cada perfil de firewall tem seu próprio conjunto de regras de firewall ativas. Para exibir as regras:

a. Na página principal, clique em Configurações.

b. Selecione Conexões de rede > Firewall.

c. Clique na guia Regras.

d. Ao lado de Perfil atual de firewall, selecione o perfil de firewall adequado.

É possível ver uma lista de regras, que contém as seguintes informações:

Campo	Descrição
Em uso	Se a caixa de seleção estiver marcada, a regra está ativada no momento. Se a caixa de seleção estiver vazia, a regra está desativada no momento.
Nome	Nome da regra. Há dois tipos de regras: ○ Regras predefinidas: Estas regras são mostradas em cinza. Elas foram predefinidas para o *perfil de firewall* selecionado. ○ Suas próprias regras: Se você adicionou suas próprias regras, elas serão mostradas em preto sobre a linha Suas regras serão adicionadas aqui.
Tipo	Tipo de regra: ○ ✔: essa regra permite o tráfego de rede. ○ ✖: essa regra nega o tráfego de rede. ○ ! : essa regra gera alertas no registro de alertas e possivelmente mostra uma janela pop-up de alerta quando a regra permite ou nega o tráfego de rede.
Host remoto	Os *endereços IP* e as redes aos quais a regra se aplica. Se a regra se aplicar a todos os *endereços IP*, esse campo mostrará um dos seguintes valores:

	○ 0.0.0.0/0,::/0: a regra se aplica a todos os endereços *IPv4* e *IPv6*. ○ 0.0.0.0/0: a regra se aplica a todos os endereços *IPv4*. ○ ::/0: a regra se aplica a todos os endereços *IPv6*.

e. Para exibir os detalhes da regra, selecione uma regra na lista e clique em Detalhes.
   - Se a regra foi predefinida, a caixa de diálogo Detalhes da regra é aberta e exibe a regra predefinida. Após visualizar os detalhes, clique em Concluir.
   - Se você mesmo adicionou a regra, a caixa de diálogo Detalhes da regra é aberta. Clique em Próximo até um resumo da regra ser exibido. Após visualizar os detalhes, clique em Cancelar.

79. Detalhes da regra de firewall

Os detalhes da regra de firewall incluem o nome e o tipo de regra, os endereços IP e serviços aos quais a regra se aplica, e as configurações de alertas.

É possível exibir as seguintes informações na caixa de diálogo Detalhes da regra:

Campo	Descrição
Nome	O nome da regra.
Tipo	O tipo de regra, que define se ela permite ou nega o tráfego de rede.
Endereço remoto	Os *endereços IP* e as redes aos quais a regra se aplica. Se a regra se aplicar a todos os *endereços IP*, o campo mostra um dos seguinte valores: • 0.0.0.0/0,::/0: a regra se aplica a todos os endereços *IPv4* e *IPv6*. • 0.0.0.0/0: a regra se aplica a todos os endereços *IPv4*. • ::/0: a regra se aplica a todos os endereços *IPv6*.
Serviços	A coluna Serviço mostra os *serviços de firewall* que a regra inclui. A coluna Direção mostra se a regra se aplica aos serviços de entrada (entr.), serviços de saída (saída) ou ambos.
Alertando	Mostra se a regra gera alertas e mostra janelas pop-up de alertas.
Texto de alerta	Se a regra gerar alertas, mostra o texto que é exibido no registro de alertas e na janela pop-up.

80. O que são serviços de firewall

Os serviços de firewall definem o tipo de tráfego ao qual uma regra de firewall se aplica.

Os serviços de rede, como navegação na web, compartilhamento de arquivos ou acesso ao console remoto, são exemplos desses serviços de firewall.

Um serviço usa determinados protocolo e porta. Por exemplo, o serviço HTTP usa o protocolo TCP e a porta de número 80.

Um serviço de firewall usa dois tipos de portas:

- Porta de início: a porta no computador que inicia a conexão.
- Porta de resposta: a porta no computador onde termina a conexão.

O que determina se a porta em seu computador é uma porta de início ou uma porta de resposta é a direção do tráfego:

- Se o serviço de firewall for para o tráfego de saída, a porta de início será a porta no seu computador. A porta de resposta será então a porta em um computador remoto.
- Se o serviço de firewall for para o tráfego de entrada, a porta de início será a porta em um computador remoto. A porta de resposta será então a porta em seu próprio computador.

As portas de resposta são geralmente mencionadas na documentação do software. Em geral, a porta de início pode ser qualquer porta superior a 1023. Entretanto, você talvez precise definir portas de início específicas para alguns jogos. Se esse for o caso, elas também serão mencionadas na documentação do software.

Se você criar uma nova regra de firewall, poderá adicionar vários serviços predefinidos à regra. Você também poderá criar e adicionar seus próprios serviços se o que você precisar não estiver na lista.

81. Ver serviços de firewall

Você pode exibir os serviços de firewall existentes na guia Serviços.

Para exibir os serviços:

a. Na página principal, clique em Configurações.

b. Selecione Conexões de rede > Firewall.

c. Clique na guia Serviços. É possível exibir as seguintes informações:

Campo	Descrição
Nome	Nome do serviço.
Usado na regra	Nome da regra de firewall na qual o serviço foi usado.

d. Para exibir os detalhes de um serviço, selecione o serviço na lista e clique em Detalhes. A caixa de diálogo Detalhes do serviço é aberta.

e. Após exibir os detalhes do serviço, clique em Fechar.

82. O que são regras de firewall dinâmicas

As regras de firewall dinâmicas são criadas para conexões entre computadores remotos e programas de servidores no seu computador.

Se uma janela pop-up do controle de aplicativos for mostrada e você permitir uma conexão de entrada, por exemplo, para um programa de servidor ponto a ponto em seu computador, o firewall cria uma regra de firewall dinâmica temporária. Esta regra será adicionada à lista de regras dinâmicas da guia Atividade. A regra abre uma porta para este programa e a mantém aberta enquanto o programa monitorar a porta por conexões de entrada.

Quando o programa para de monitorar a porta, a regra fecha a porta e a regra dinâmica é removida da lista de regras dinâmicas. Dependendo das configurações do controle de aplicativos, as janelas pop-up do controle de aplicativos talvez não sejam mostradas para todos os programas. Se a janela pop-up não for mostrada, uma regra de firewall dinâmica será criada automaticamente para o programa.

83. Ver regras de firewall

A guia Atividade mostra as regras de firewall dinâmicas que estão ativas no momento.

As regras de firewall dinâmicas são criadas para as conexões entre computadores remotos e os programas de servidor do seu computador.

Para ver as regras de firewall dinâmicas:

a) Na página principal, clique em Configurações.

b) Selecione Conexões de rede > Firewall.

c) Clique na guia Atividade. É possível exibir as seguintes informações:

- Aplicativo: o nome do arquivo do programa de servidores do seu computador que atualmente monitora conexões de entrada em uma porta.
- Porta de monitoramento: a porta que a regra de firewall dinâmica abriu. O programa de servidores monitora as conexões de entrada dessa porta.
- Endereço remoto: o programa de servidores monitora as conexões da porta a partir dos seguintes endereços IP:
  - 0.0.0.0/0: Todos os endereços IPv4.
  - ::/0: Todos os endereços IPv6.

84. Como funcionar a ordem de prioridade das regras de firewall

As *regras de firewall* possuem uma ordem de prioridade que determina a ordem na qual as regras são aplicadas ao tráfego de rede.

As *regras de firewall* são mostradas como uma lista na guia Regras . As *regras* serão aplicadas de cima para baixo e a primeira regra que corresponder ao tráfego substituirá todas as outras regras seguintes. O princípio mais importante é permitir somente o tráfego necessário e bloquear o restante. Portanto, a última regra de um *perfil de firewall* é a regra Negar o restante. Essa regra bloqueia todo o tráfego que as regras anteriores não permitem especificamente.

As *regras de firewall* dinâmicas são mostradas separadamente como uma lista na guia Atividade . A prioridade das regras dinâmicas é menor do que a prioridade das *regras de firewall* normais. Isso significa que se uma *regra de firewall* negar algum tráfego, a regra dinâmica não poderá permiti-lo. No entanto, a prioridade das regras dinâmicas é maior do que a prioridade predefinida na regra Negar o restante.

85. Um exemplo de como funciona a ordem de prioridade

- Você adicionou uma regra que nega todo o tráfego de saída do *FTP*. Acima da regra na lista de regras, você adiciona outra regra que permite uma conexão *FTP* com seu endereço IP do provedor de serviços. Essa regra permite que você crie uma conexão *FTP* com esse endereço IP.
- Você criou uma regra que permite que você crie uma conexão *FTP* com o seu endereço IP do provedor de serviços. Acima da regra na lista de regras, você adiciona outra regra que nega todo o tráfego do *FTP*. Essa regra impede que você

crie uma conexão *FTP* com o endereço IP do seu provedor de serviços da internet (ou com qualquer outro endereço IP).

86. Como permitir ou bloquear tráfego de rede por meio do firewall

Você pode permitir ou bloquear o tráfego de rede usando regras de firewall.

87. O que fazer se um alerta do firewall for exibido

Uma janela pop-up de alerta do firewall é exibida na tela de seu computador quando o firewall detecta tráfego de rede suspeito no seu computador.

Uma janela pop-up é exibida quando os pop-ups de alerta foram ativados e ocorre o seguinte:

- o tráfego corresponde a uma das regras de firewall atuais e o alerta foi ativado para essa regra ou
- houve uma tentativa de invasão no computador e o alerta foi ativado para a Prevenção contra intrusões.

Não é necessariamente preciso fazer coisa alguma, pois o firewall bloqueia o tráfego suspeito automaticamente e impede as tentativas de invasão (se a opção "Bloquear e registrar tentativa" foi ativada nas configurações da prevenção contra intrusões).

Se uma janela pop-up de alerta for exibida, proceda da seguinte maneira:

a) Leia as informações sobre o alerta.

b) Para exibir os detalhes do alerta, clique em Detalhes >>.

c) Se você não quiser que janelas pop-up de alertas do firewall sejam mostradas, selecione a caixa de seleção Não mostrar este alerta novamente.

d) Para obter mais informações sobre o endereço IP remoto, clique em Nome DNS. Mostra o nome de domínio do Endereço IP, por exemplo, www.exemplo.com. Se o nome de domínio não puder ser resolvido, o botão Nome DNS torna-se indisponível e nenhum nome de domínio é exibido.

e) É possível criar uma nova regra de firewall para o tráfego que gerou o alerta. Essa regra permite ou nega esse tipo de tráfego posteriormente. Clique em Criar regra e preencha as informações sobre a regra.

f) Para fechar a caixa de diálogo Alertas do firewall, clique em Fechar.

Agora você pode continuar a usar o computador normalmente.

88. Ativar e desativar os alertas de firewall:

Você pode selecionar se as pop-ups de alerta do firewall são mostradas.

Para ativar e desativar as janelas pop-up de alerta:

a) Na página principal, clique em Configurações.

b) Selecione Conexões de rede > Firewall.

c) Clique na guia Configurações.

d) Clique em Registro de alerta.

e) Para ativar as janelas pop-up, marque a caixa de seleção Mostrar pop-ups de alerta. Para desativar as janelas pop-up, desmarque a caixa de seleção.

f) Clique em Fechar.

Se você ativou as janelas pop-up, uma delas será exibida na próxima vez que houver correspondência entre algum tráfego e as regras de firewall atuais. Isso se aplica somente às regras que possuem o registro de alertas e as janelas pop-up ativas. Se você desativou as janelas pop-up, elas não serão exibidas novamente.

89. Como criar regras e serviços de firewall

É possível criar as suas próprias regras e serviços de firewall para permitir ou negar parte do tráfego da internet.

Antes de começar a criar uma regra, selecione o perfil de firewall para o qual deseja adicionar esta regra.

Nota: Você talvez não consiga adicionar suas próprias regras a todos os perfis de firewall.

90. Criar um serviço de firewall

Pode ser necessário criar um novo serviço de firewall, por exemplo, se você começar a usar um novo programa que precisa conectar-se à internet e que não possui um serviço predefinido.

O serviço define os protocolos e as portas que o programa usa. Para obter mais informações, consulte a documentação do programa.

Para criar um serviço de firewall:

a) Na página principal, clique em Configurações.

b) Selecione Conexões de rede > Firewall.

c) Clique na guia Serviços.

d) Clique em Adicionar. A caixa de diálogo Adicionar novo serviço é aberta.

e) No campo Nome, insira um nome para o serviço. Use um nome que você possa identificar facilmente.

f) Na lista Protocolo, selecione o protocolo para o serviço:

- ICMP (1)
- TCP (6)
- UDP (17)

Para usar outro protocolo IP, insira o número do protocolo (0-255) no campo.

g) Se o serviço usar o protocolo TCP ou UDP, defina as portas de início para o serviço. Se a documentação do programa não incluir as portas de início, você geralmente pode usar qualquer número de porta acima de 1023.

- Próximo ao campo Portas do iniciador, clique em Editar.
- Adicione as portas:
  - Para inserir uma única porta, digite o número da porta no campo Única, por exemplo, 1024.
  - Para inserir um intervalo de portas, adicione o número de porta mais alto e mais baixo do intervalo nos campos Intervalo&, por exemplo, 1024-65535.
- Clique em Adicionar à Lista.
- Repita as etapas de "a" a "c" para adicionar todas as portas necessárias.
- Clique em OK.

h) Se o serviço usar o protocolo TCP ou UDP, defina as portas de resposta para o serviço. As portas de resposta são geralmente mencionadas na documentação do programa.

- Ao lado do campo Portas do respondedor, clique em Editar.
- Adicione as portas:
  - Para inserir uma única porta, digite o número da porta no campo Única.
  - Para inserir um intervalo de porta, adicione a porta mais alta e mais baixa do intervalo nos campos Intervalo.
- Clique em Adicionar à Lista.

- Repita as etapas de "a" a "c" para adicionar todas as portas necessárias.
- Clique em OK.

i) Se o serviço usar o protocolo ICMP, defina o tipo e código ICMP para o serviço. Clique em Editar para inserir os valores nos campos Tipo e Código. Os valores permitidos são 0-255.

j) Se você for usar esse serviço para permitir o tráfego de entrada, poderá definir se deseja permitir também o tráfego de difusão e multi difusão. Esse tipo de tráfego é criado por programas de fluxo, como rádio e televisão na web. Para permiti-lo, marque as caixas de seleção Permitir difusões e Permitir difusões múltiplas. Geralmente, você pode deixar essas caixas de seleção desmarcadas.

k) Na caixa de diálogo Adicionar novo serviço, clique em OK.

O seu novo serviço será mostrado na lista de serviços na guia Serviços. Para permitir ou negar o tráfego que o serviço define, é necessário adicionar o serviço a uma regra de firewall que permita conexões de saída da Internet.

91. Iniciar a criação de uma regra

Insira um nome para a regra e selecione se a regra de firewall deve negar ou permitir o tráfego.

Para iniciar a criação de uma regra:

a) Na página principal, clique em Configurações.

b) Selecione Conexões de rede > Firewall.

c) Clique na guia Regras.

d) Clique em Adicionar. A caixa de diálogo Adicionar nova regra é exibida.

e) No campo Nome, insira um nome para a regra. Use um nome que você possa identificar facilmente.

f) Para negar ou permitir tráfego, selecione Negar ou Permitir.

g) Para criar uma regra que seja válida somente quando você possuir uma conexão discada ativa, selecione Usar esta regra somente com conexão telefônica. Esta opção é relevante apenas se você usar um modem ou ISDN para sua conexão à internet. Marque essa opção, por exemplo, se você usar um laptop fora de sua rede doméstica e acessar a internet por meio de um modem ou de uma conexão

ISDN. Fora de sua casa, o laptop não estará protegido pelo firewall do roteador e você talvez deva criar uma regra mais rígida que negue todo o tráfego de entrada desnecessário e usar essa regra quando estiver fora de casa. Geralmente, você não precisa criar uma regra, e o perfil de firewall padrão protege o seu computador tanto dentro quanto fora de casa.

h) Clique em Próximo.

92. Selecionar os endereços IP

Aplique a regra a todas as conexões de rede ou especifique os *endereços IP* e redes aos quais as novas regras se aplicam.

Nota: As opções relacionadas a endereços IPv6 estão disponíveis apenas se o seu sistema operacional for o Microsoft Windows Vista ou o Windows 7.

Para selecionar os *endereços IP*:

a) Selecione uma das seguintes opções:

- Para aplicar a regra a ambos os endereços, *IPv4* e *IPv6*, selecione Qualquer endereço IP.
- Para aplicar a regra a todos os endereços *IPv4*, selecione Qualquer endereço *IPv4*.
- Para aplicar a regra a todos os endereços *IPv6*, selecione Qualquer endereço *IPv6*.
- Para aplicar a regra a *endereços IP* e redes específicas, selecione Personalizar e clique em Editar. A caixa de diálogo Endereços será aberta.

b) Na caixa de diálogo Endereços, selecione uma das opções a seguir na lista Tipo:

Tipo	Exemplo de endereço
Endereço IP	192.168.5.16
Nome *DNS*	www.exemplo.com
Faixa *IP*	192.168.1.1-192.168.1.63
Sub-rede IP	192.168.88.0/29
MeuDNS	[meudns]

MinhaRede	[minharede]
Endereço *IPv6*	2001:db8:85a3:8d3:1319:8a2e:370:733
Intervalo de *IPv6*	2001:db8:1234:: - 2001:db8:1234:FFFF:FFFF:FFFF:FFFF:FFFF
Sub-redeIPv6	2001:db8:1234::/48

c) Insira o endereço no campo Endereço.

d) Para adicionar o endereço à lista de endereços, clique em Adicionar à Lista.

e) Repita as etapas de "a" a "c" para adicionar todos os endereços necessários à lista de endereços.

f) Clique em OK.

g) Clique em Próximo.

93. Como posso definir uma sub-rede IP?

Para definir uma *sub-rede* IP, use a notação *Roteamento entre domínios sem classe* (CIDR, Classless Inter-Domain Routing). Essa é uma notação padrão que consiste de um *endereço de rede* e uma *máscara de sub-rede*. Por exemplo:

Endereço de rede	Máscara de sub-rede	Notação CIDR
192.168.0.0	255.255.0.0	192.168.0.0/16
192.168.1.0	255.255.255.0	192.168.1.0/24
192.168.1.255	255.255.255.255	192.168.1.255/32

94. Selecione os serviços e direção:

Selecione os serviços aos quais a regra de firewall se aplica e a direção do tráfego.

Para selecionar os serviços e a direção:

a) Selecione os serviços aos quais você deseja aplicar a regra:

- Para aplicar a regra a todo o tráfego de IP, selecione Todo o tráfego IP na lista.
- Se o serviço que você precisa não estiver na lista, crie-o primeiro.
- O ícone é exibido na coluna Direção para os serviços selecionados.

b) Para cada serviço, selecione a direção do tráfego ao qual a regra se aplica. A direção é do computador para a Internet ou vice-versa. Para selecionar a direção, clique no ícone na coluna Direção.

Direção	Explicação
	O serviço é permitido ou negado em ambas as direções.
	O serviço é permitido ou negado se for da Internet para o seu próprio computador (entrada).
	O serviço é permitido ou negado se for do seu próprio computador para a Internet (saída).

c) Clique em Próximo.

95. Selecionar opções de alerta

Selecione como o produto o notifica quando a regra de firewall nega ou permite o tráfego.

Para selecionar a opção de alerta:

a) Selecione uma das seguintes opções:

- Para não ser notificado, selecione Sem alerta. Os alertas não serão gerados no registro de alertas e nenhuma janela pop-up de alerta será exibida. Recomendamos que você selecione essa opção se estiver criando uma regra para permitir o tráfego.
- Para que o produto gere alertas no registro de alertas, selecione Registrar.
- Para que o produto gere alertas no registro de alertas e para que as janelas pop-up de alerta sejam mostradas, selecione Registrar e alertar. Observe que é necessário ativar as janelas pop-up de alerta também na caixa de diálogo Alertas do firewall.
- No campo Texto de Alerta, insira uma descrição a ser mostrada no registro de alertas e nas janelas pop-up.

b) Clique em Próximo.

96. Verificar e aceitar a regra

Verifique e aceite a nova regra.

Para fazer isso:

a) Verifique o resumo da regra. Se for necessário editar a regra, clique em Anterior.

b) Quando estiver satisfeito com a nova regra, clique em Concluir.

A sua nova regra será mostrada na lista de regras na guia Regras e será ativada automaticamente. Se você criou várias regras, poderá definir suas ordens de prioridade.

97. Definir a ordem de prioridade das regras de firewall

Se você criou várias regras de firewall novas, defina suas ordens de prioridade.

Você talvez queira fazer isso, por exemplo, se uma regra negar algum tráfego que você deseja permitir. Nesse caso, é necessário criar uma nova regra de "permissão" e mover essa regra acima da regra de "negação". Dessa forma, a regra de "permissão" é aplicada primeiro ao tráfego. É possível alterar a ordem de prioridade somente dessas regras que você mesmo criou.

Para definir a ordem de prioridade:

a) Na página principal, clique em Configurações.

b) Selecione Conexões de rede > Firewall.

c) Clique na guia Regras.

d) Clique na regra que deseja mover e, com o botão do mouse pressionado, arraste a regra para o novo local na tabela.

As regras agora serão aplicadas ao tráfego de acordo com a nova ordem de prioridades.

98. Como abrir uma porta por meio do firewall

É possível abrir uma porta por meio do firewall se desejar permitir algum tráfego da internet e se souber o número da porta que deseja abrir.

Talvez não seja possível adicionar suas próprias regras a todos os perfis de firewall. Selecione o perfil de firewall para o qual deseja adicionar a nova regra antes de abrir a porta.

Você cria uma nova regra de firewall e dois serviços novos sempre que uma porta é aberta por meio do firewall.

a) Na página principal, clique em Tarefas.
b) Clique em Abrir porta de firewall.
c) No campo Nome, digite um nome para a nova regra de firewall.
d) No campo Número da porta, defina a porta de resposta para a regra. A porta de resposta é geralmente citada na documentação do produto.
e) Clique em OK.

A nova regra foi adicionada às regras do firewall e dois serviços novos foram criados na lista dos serviços de firewall para ambos os protocolos TCP e UDP com o número da porta específico.

99. Exemplos de criação de regras de firewall

É possível criar uma nova regra de firewall para jogar um novo jogo em rede ou para compartilhar arquivos em sua rede doméstica.

100. Criar uma regra para jogo de rede

Este é um exemplo de como criar serviços de firewall e uma regra de firewall para um jogo de rede imaginário nomeado Jogo_1.

Para criar os serviços de firewall, você precisa saber quais são os protocolos que o jogo usa. Precisa também saber quais são as portas que o jogo usa para as conexões de entrada do servidor de jogos para o computador. Nesse caso, eles são:

Protocolo	Tipo de porta	Local	Portas
UDP	De início	Servidor de jogos	1024
UDP	De resposta	Próprio computador	8889, 9961
TCP	De início	Servidor de jogos	1025
TCP	De resposta	Próprio computador	17475, 9961

Nota: Não é necessário criar os serviços de firewal ou uma regra de firewall para as conexões de saída do seu computador para o servidor de jogos.

Para criar os serviços e uma regra para as conexões de entrada:

a) Adicione os novos serviços da seguinte maneira:

Etapa	Exemplo
Insira um nome para o primeiro serviço	Service_Game_1_UDP
Selecione o *protocolo*	*UDP*
Insira as *portas de início*	1024
Insira as *portas de resposta*	8889, 9961
Insira um nome para o segundo serviço	Service_Game_1_TCP
Selecione o segundo *protocolo*	*TCP*
Insira as *portas de início*	1025
Insira as *portas de resposta*	17475, 9961

b) Depois que você adicionar os serviços, eles serão mostrados na lista de serviços.

c) Adicione uma nova regra de firewall da seguinte maneira:

Etapa	Exemplo
Insira um nome para a regra	Rule_Game_1
Selecione o tipo de regra	Permitir
Selecione os *endereços IP*	Qualquer endereço
Selecione os serviços	Service_Game_1_UDP, Service_Game_1_TCP
Selecione a direção	(da internet para o computador)
Selecione o tipo de *alerta*	Sem *alerta*

Depois que você adicionar a regra, ela ficará ativa e será mostrada na lista de regras.

101. Criar uma regra para compartilhar arquivos em uma rede doméstica

Este é um exemplo de como criar uma nova regra de firewall para que o compartilhamento de arquivos do Windows compartilhe arquivos entre computadores em sua rede doméstica.

Se você usar um roteador em sua rede, verifique as configurações do DHCP (Dynamic Host Configuration Protocol) do roteador para saber qual é o intervalo de endereço IP alocado para sua rede doméstica. Para obter mais informações, consulte a documentação do roteador.

O intervalo de Endereço IP mais utilizado para redes domésticas é 192.168.1.1 - 192.168.1.254. Para compartilhar arquivos entre todos os computadores, é necessário criar a mesma regra em todos os computadores.

Para criar a regra:

a) Na página principal, clique em Configurações.

b) Selecione Conexões de rede > Firewall.

c) Clique na guia Regras.

d) Clique em Adicionar.

e) Insira um nome e selecione o tipo de regra:

Etapa	Exemplo
Insira um nome para a regra	Compartilhamento de arquivo
Selecione o tipo de regra	Permitir

f) Selecione os endereços IP:

Etapa	Exemplo
• Clique em Personalizar. • Clique em Editar. • Selecione *IP* intervalo e insira os endereços dos computadores no campo. • Clique em Adicionar à Lista.	192.168.1.1 - 192.168.1.254

g) Selecione os serviços e direção:

Etapa	Exemplo
Selecione os serviços que o compartilhamento de arquivos do Windows usa	○ SMB sobre TCP/IP (TCP) ○ SMB sobre TCP/IP (UDP) ○ Compartilhamento de arquivos e de impressoras de rede do Windows ○ Navegação na rede do Windows ○ ICMP / Internet Control Message Protocol
Selecione a direção de ambos os serviços	(da Internet para o computador)

h) Selecione o tipo de alerta:

Etapa	Exemplo
Selecione o tipo de alerta	Sem *alerta*

i) Verifique o resumo da regra e clique em Concluir. A sua nova regra será mostrada na lista de regras na guia Regras e será ativada automaticamente.

j) Faça um teste para verificar se a regra funciona. Para fazer isso, use o compartilhamento de arquivos do Windows para compartilhar uma pasta ou um arquivo e verifique se é possível acessar a pasta ou o arquivo a partir de todos os computadores.

Dica: Para compartilhar a impressora em sua rede doméstica, crie uma regra semelhante. Nesse caso, você precisará criar somente uma regra de "permissão" de entrada no computador ao qual a impressora está conectada.

102. Ativar e desativar uma regra de firewall

Você pode desativar uma regra de firewall para permitir temporariamente algum tráfego negado pela regra.

Você pode ativar ou desativar as regras que você mesmo criou.

Para ativar ou desativar uma regra:

a) Na página principal, clique em Configurações.

b) Selecione Conexões de rede > Firewall.

c) Clique na guia Regras.

d) Proceda de uma das seguintes maneiras:

- Para desativar uma regra, desmarque a caixa de seleção na coluna Em uso.
- Para ativar a regra, marque a caixa de seleção.

Dependendo do que você selecionar, a regra de firewall ficará ativada ou desativada.

103. Alterar uma regra de firewall

Você pode alterar somente uma regra de firewall que você mesmo tenha criado.

Para alterar uma regra:

a) Na página principal, clique em Configurações.
b) Selecione Conexões de rede > Firewall.
c) Clique na guia Regras.
d) Selecione a regra e clique em Detalhes. A caixa de diálogo Detalhes da regra é aberta.
e) Faça as alterações necessárias em cada etapa e vá para a próxima etapa clicando em Próximo.
f) Na caixa de diálogo Detalhes da regra, verifique as alterações feitas.
g) Se estiver satisfeito com a regra, clique em Concluir.

As alterações feitas são aplicadas à regra.

104. Configurações do firewall

Na guia Configurações, é possível alterar as configurações do IPv6 e o nível de alerta e permitir todo o tráfego entre computadores em uma rede doméstica.

A guia Configurações também contém o campo Bloquear fragmentos IP menores que. O firewall bloqueia os fragmentos do pacote IP que são mais curtos do que o limite recomendado mostrado nesse campo. Os fragmentos curtos de pacote IP podem indicar um ataque de fragmentação, que pode fazer com que o computador trave. Recomendamos que o limite não seja alterado nesse campo.

105. Alterar as configurações do IPv6

Na guia Configurações, você pode definir como o firewall lida com o tráfego do IPv6.

Se o seu sistema operacional for o Microsoft Windows Vista ou o Windows 7, você pode bloquear todo o tráfego do IPv6 ou aplicar regras de firewall normais ao tráfego. Se você usar algum outro sistema operacional, poderá somente bloquear ou permitir todo o tráfego do IPv6.

Para alterar as configurações do IPv6:

a) Na página principal, clique em Configurações.
b) Selecione Conexões de rede > Firewall.
c) Clique na guia Configurações.
d) Para definir como o firewall lida com o tráfego do IPv6, selecione uma das seguintes opções na lista Selecione opções de filtragem de tráfego IPv6:

- Se você usar o Microsoft Windows Vista ou o Windows 7:
  - Bloquear: bloqueia todo o tráfego do IPv6.Recomendamos que você mantenha essa opção selecionada.
  - Normal: As regras de firewall normais definem se o tráfego de IPv6 é permitido ou bloqueado. Você talvez deva selecionar essa opção se estiver usando o protocolo IPv6 em seu computador.
- Se você usar algum outro sistema operacional:
  - Bloquear: todo o tráfego do IPv6 é bloqueado. Recomendamos que você mantenha essa opção selecionada.
  - Permitir: permite todo o tráfego do IPv6.Você talvez deva selecionar essa opção se estiver usando o protocolo IPv6 em seu computador.

Nota: Permitir todo o tráfego do IPv6 é um risco à segurança, pois nenhuma regra de firewall é aplicada ao tráfego do IPv6.

e) Clique em OK.

As alterações feitas nas configurações do IPv6 agora estão ativas.

106. O que fazer se você compartilhar uma conexão à internet

Para compartilhar uma conexão à internet em seu computador com as outras redes em sua casa, é necessário permitir todo o tráfego entre estes computadores através do firewall.

Nota: Permita todo o tráfego através do firewall somente se você usar o Windows Internet Connection Sharing. Para compartilhar outros recursos, como unidades, arquivos ou impressoras, recomendamos que você crie novas regras de firewall para esse objetivo.

Você pode permitir todo o tráfego através do firewall definindo a conexão entre a rede doméstica e o computador e a conexão entre o computador e a internet como confiável. Você pode definir uma *interface de rede confiável*, se:

- Você possui um computador com uma conexão à internet.

- Este computador tem duas *placas de interface de rede*: Uma para conexão à internet e outra para conexão à rede doméstica.
- Você ativou o Windows Internet Connection Sharing no computador que tem a conexão à Internet.
- Você instalou nosso programa com um firewall em todos os seus computadores. Isso garante que é seguro definir uma interface confiável entre os computadores.

Para definir a interface de rede confiável, é necessário selecionar a placa de interface de rede (adaptador) que conecta o computador à rede doméstica.

Para selecionar a placa de interface de rede no computador com a conexão à Internet:

a) Na página principal, clique em Configurações.

b) Selecione Conexões de rede > Firewall.

c) Clique na guia Configurações.

d) Na lista Adaptador de rede confiável, selecione a *placa de interface de rede* (adaptador) que conecta o seu computador à rede doméstica. O *endereço IP* do computador será mostrado no campo *Endereço IP*.

Nota: Como o *firewall* permite todo o tráfego através da interface de rede selecionada, não selecione a opção confiável como a interface da internet. Se fizer isso, o firewall deixará de proteger o computador.

e) Clique em OK.

O *firewall* agora permite todo o tráfego entre o computador com a conexão à Internet e à rede doméstica, e você pode usar a Internet de todos os computadores.

107. E se eu usar uma placa de TV digital?

Se você usar uma placa de TV digital e a imagem da televisão congelar, pode ser necessário definir a interface para a televisão como confiável.

108. Como controlar aplicativos de rede

O controle de aplicativos impede que programas perigosos conectem-se à internet.

O controle de aplicativos protege principalmente contra as ameaças externas que são causadas pelos programas em seu computador. Geralmente, quando um programa

tenta conectar-se à internet, o controle de aplicativos mostra uma janela pop-up. Nessa janela é possível permitir ou negar a conexão:

- Se você acreditar que o programa é seguro, poderá permitir a conexão. Por exemplo, o programa pode ser considerado seguro se você mesmo acabou de abri-lo. Quando você permite a conexão, o *firewall* abre uma *porta* para o programa e permite a conexão pelo tempo que ele estiver aberto. Quando você fecha o programa, o firewall fecha a *porta*.
- Se você não confiar no programa, deverá negar a conexão. Por exemplo, é possível que um programa não seja seguro se você não reconhecê-lo ou se não foi você mesmo que o instalou.

Dependendo das suas configurações do controle de aplicativo, as pop-ups do controle de aplicativo talvez não sejam mostradas para programas que o DeepGuard considera seguros. Estes programas têm permissão para conectar-se à internet automaticamente.

O controle de aplicativos também pergunta se você deseja permitir que os programas em seu computador conectem-se à internet. Isso acontece, por exemplo, se você usar o Skype.

Nota: Se um programa não funcionar em seu computador, não desative o controle de aplicativos. Se fizer isso, o nível de proteção do computador será reduzido. Em vez disso, altere as configurações do controle de aplicativos ou das *regras de firewall*.

109. Qual é a diferença entre o firewall e o controle de aplicativos

Um firewall fornece proteção geral em nível de rede, enquanto o controle de aplicativos permite que você controle o uso de programas específicos. O firewall protege contra ameaças que são causadas por conexões da internet para seu computador (entrada). O firewall permite ou não as conexões com base em protocolos e endereços IP usados pela conexão.

O controle de aplicativos protege você principalmente contra ameaças que são provocadas por conexões do seu computador para a internet (saída). O controle de aplicativos permite ou não conexões com base nos programas que criam a conexão.

110. O que fazer se uma janela pop-up do controle de aplicativos for exibida

Se uma janela pop-up do controle de aplicativos for exibida, você deverá decidir se permite ou nega uma tentativa de conexão para o programa que é mostrado na janela pop-up.

As janelas pop-up do controle de aplicativos podem indicar atividades maliciosas, como cavalos de tróia, worms ou spyware. Por outro lado, as janelas pop-up também são mostradas quando você usa os programas do seu computador normalmente.

Para permitir ou negar uma tentativa de conexão:

a) Verifique as informações sobre a tentativa de conexão na janela pop-up.

b) Para exibir os detalhes da tentativa de conexão, como o nome do programa e o endereço IP do computador remoto, clique em Detalhes.

c) Para que as janelas pop-up sobre este programa não sejam mostradas novamente, marque a caixa de diálogo Não mostrar esta caixa de diálogo para este programa novamente.

d) Permitir ou negar a conexão:

- Clique em Permitir se tiver certeza de que a tentativa de conexão é segura. Permita a conexão nas seguintes circunstâncias:

Tipo de janela pop-up	Descrição	Clique em Permitir se...
Nova tentativa de conexão (de saída)	Um programa *cliente* em seu computador está tentando conectar-se à Internet.	Você mesmo iniciou este programa pela primeira vez.
Aplicativo alterado (de saída)	Um programa *cliente* em seu computador está tentando conectar-se à internet, mas foi alterado desde a conexão anterior.	O programa foi atualizado em seu computador desde a última vez que foi usado.
Novo aplicativo de servidor (de entrada)	Um programa em seu computador está tentando agir como um *servidor* e deseja iniciar o monitoramento por conexões de entrada.	Você mesmo iniciou o programa de *servidor* em seu computador.
Aplicativo alterado (de entrada)	Um programa de *servidor* em seu computador deseja iniciar o monitoramento para conexões de entrada, mas foi alterado desde a tentativa de conexão anterior.	O programa de *servidor* foi atualizado em seu computador desde a última vez que foi usado.

- Clique em Negar se não tiver certeza de que a tentativa de conexão é segura.

Dependendo da ação selecionada, a conexão será permitida ou negada. Se você marcou a caixa de seleção Não mostrar esta caixa de diálogo para este programa novamente, o programa será adicionado à lista de programas permitidos ou negados da guia Aplicativos . Nenhuma janela pop-up será mostrada novamente sobre as tentativas de conexão deste programa.

111. Programas seguros e inseguros e tentativas de conexão

Antes de permitir uma conexão em uma janela pop-up do controle de aplicativos, verifique se o programa é seguro.

112. Quais programas e tentativas de conexão podem ser considerados seguros

- Um programa conhecido que você mesmo iniciou.
- O sistema operacional Microsoft Windows, que se conecta à internet para obter serviços de atualização.

113. Quais programas e tentativas de conexão podem não ser considerados seguros

- Qualquer programa recebido de uma origem desconhecida.
- Qualquer programa que não foi instalado por você ou que você não reconheça.
- Qualquer programa que você considera seguro, mas que tenta conectar-se à internet ou age como um *servidor* sem que você o tenha iniciado.

114. Permitir ou negar conexões para programas:

É possível permitir ou negar conexões à internet para programas na guia Aplicativos.

Você pode, por exemplo, permitir uma conexão a um programa que você tenha negado, sem intenção, em uma janela pop-up do controle de aplicativos.

Por padrão, a guia Aplicativos mostra os seguintes programas:

- Quando a opção Avisar sobre novos programas está ativada: programas, que você permitiu ou negou e para os quais selecionou a opção Não mostrar esta caixa de diálogo para este programa novamente em uma janela pop-up do controle de aplicativos.

- Quando a opção Permitir e adicionar à lista de programas está ativada: programas permitidos.
- Os programas que você adicionou manualmente à lista de programas desta guia.

Esta guia não mostra programas do sistema operacional permitidos automaticamente ou programas que o DeepGuard considera seguro.

Para permitir ou negar a conexão para um programa:

a) Na página principal, clique em Configurações.

b) Selecione Conexões de rede > Controle de Aplicativos.

c) Clique na guia Aplicativos.

d) Selecione o programa e clique em Detalhes. A caixa de diálogo Detalhes do aplicativo é aberta.

e) Em Conexão de saída (cliente), selecione a opção apropriada:
   - Negar: para negar a conexão do programa à Internet na próxima vez que ele for iniciado.
   - Permitir: para permitir a conexão do programa à Internet na próxima vez que ele for iniciado.
   - Solicitar: para que uma janela pop-up do controle de aplicativos seja mostrada na próxima vez que o programa tentar conectar-se à internet. Nessa janela pop-up, você pode permitir ou negar a conexão.

f) Em Servidor (Entrada), selecione a opção apropriada:
   - Negar: para negar conexões da internet para o programa.
   - Permitir: para permitir conexões da internet para o programa.
   - Solicitar: para que a janela pop-up do controle de aplicativos seja mostrada na próxima vez que houver uma tentativa de conexão da Internet para esse programa. Nessa janela pop-up, você pode permitir ou negar a conexão.

g) Clique em OK.

Dica: Você pode permitir ou negar conexões com a internet a um novo programa mesmo antes de começar a usá-lo. Você pode fazer isso clicando no botão Adicionar e selecionando o arquivo de programas. Depois disso, permita ou negue as conexões de entrada e saída para este programa.

115. Ativar e desativar pop-ups do controle de aplicativos

É possível ativar ou desativar as janelas pop-up do controle de aplicativos.

Se você desativar as janelas pop-up do controle de aplicativos, o produto permitirá automaticamente conexões para todos os programas.

Para ativar ou desativar as janelas pop-up do controle de aplicativos.

a) Na página principal, clique em Configurações.

b) Selecione Conexões de rede > Controle de Aplicativos.

c) Clique na guia Configurações.

d) Selecione uma das seguintes opções:

- Permitir e adicionar à lista de programas: selecione essa opção para desativar as janelas pop-up do Controle de aplicativos. O produto permite as conexões para todos os programas automaticamente.
- Avisar sobre novos programas: selecione essa opção para ativar as janelas pop-up do controle de aplicativos. Uma janela pop-up será exibida na primeira vez que um novo programa tentar abrir uma conexão.

e) Se você não quiser que as janelas pop-up do controle de aplicativos sejam mostradas para programas que o DeepGuard considera seguros, selecione Não perguntar sobre programas conhecidos. Recomendamos que você mantenha essa caixa de seleção marcada.

f) Clique em OK.

Dependendo do que você selecionar, as janelas pop-up do controle de aplicativos ficarão ativadas ou desativadas.

116. O que fazer se um programa parar de funcionar

Se você começar a usar um novo programa, por exemplo, um jogo de rede, ele poderá parar de funcionar se não conseguir conectar-se à Internet.

Isso pode ocorrer, por exemplo, pelos seguintes motivos:

- Seu perfil de firewall é muito estrito e nega conexões à internet para a maioria dos programas, incluindo os jogos em rede que estiver usando.
- Você não observou a presença de uma janela pop-up do controle de aplicativos e a janela permaneceu ativa em segundo plano.

- Você, sem intenção, negou a conexão na janela pop-up.

Para garantir que o programa possa conectar-se à Internet, proceda da seguinte maneira:

a) Na página principal, clique em Configurações.
b) Selecione Conexões de rede > Firewall.
c) Na lista Regras, verifique o perfil de firewall atual. Se for um perfil muito estrito, altere-o para outro que seja menos estrito e clique em OK.
d) Inicie o programa e verifique se está funcionando.
e) Se não estiver, desative temporariamente as janelas pop-up do controle de aplicativos a fim de permitir todas as conexões para novos programas.
f) Selecione Conexões de rede > Controle de Aplicativos.
g) Na guia Configurações, selecione Permitir e adicionar à lista de programas, e clique em OK.
h) Inicie o programa e verifique se está funcionando.
i) Se o programa funcionar, ative novamente as janelas pop-up do controle de aplicativos.
j) Selecione Conexões de rede > Controle de Aplicativos.
k) Na lista Configurações, selecione Avisar sobre novos programas, e clique em OK.

117. Como evitar intrusos

A prevenção de intrusão protege contra os ataques pela rede destinados às *portas* abertas no computador.

A prevenção contra intrusão usa regras predefinidas para reconhecer os ataques pela rede. Essas regras contêm informações sobre o tráfego malicioso conhecido. Quando a prevenção contra intrusão reconhece o tráfego que corresponde a uma regra, ela bloqueia o tráfego (se a opção "Bloquear e registrar" estiver ativada) e gera um alerta para o registro de alertas do firewall. Dependendo das suas configurações, uma janela pop-up de *alerta* do firewall pode ser exibida.

A prevenção contra intrusão reconhece e impede o tráfego malicioso causado por worms de rede, como o Sasser. O worm Sasser infecta os sistemas vulneráveis, pois envia tráfego malicioso para o serviço de compartilhamento de rede da Microsoft na porta 445 do TCP. Esse serviço é usado para compartilhar impressoras e arquivos em

uma rede. O worm abre uma conexão TCP para a porta e envia o tráfego malicioso pela porta. O tráfego inunda o sistema e pode causar, por exemplo, o travamento total do sistema.

Nota: Não desative a prevenção de intrusão. Se fizer isso, o nível de proteção do computador ficará reduzido.

118. Qual é a diferença entre o firewall e a prevenção de intrusão

A diferença entre o firewall e a prevenção de intrusão é que a prevenção bloqueia somente o tráfego que considera malicioso e permite o outro tráfego através de uma porta. O firewall ou permite ou bloqueia todo o tráfego que passa pela porta.

119. Selecionar como tentativas de intrusão são resolvidas

Na guia Prevenção de Intrusão, você pode selecionar como lidar com as tentativas de invasão.

As tentativas de invasão podem ser automaticamente bloqueadas e registradas, ou somente registradas.

Para selecionar como lidar com as tentativas de invasão:

a) Na página principal, clique em Configurações.

b) Selecione Conexões de rede > Prevenção de Intrusão.

c) Selecione uma das seguintes opções:

- Bloquear e registrar tentativa: selecione essa opção se desejar bloquear e registrar as tentativas de invasão. As tentativas são bloqueadas e as informações sobre as tentativas são exibidas na caixa de diálogo Alertas do firewall.
- Registrar: selecione essa opção se desejar registrar somente as tentativas de invasão. As informações sobre as tentativas são exibidas na caixa de diálogo Alertas do firewall.

d) Se desejar que uma pop-up Alerta do Firewall seja mostrada caso haja uma suspeita de tentativa de invasão, selecione Alertar quando tentativa de intrusão for suspeita.

e) Clique em OK.

A configuração de prevenção de intrusão foi alterada.

120. Como controlar conexões discadas

O controle de discagem impede que os programas de discador maliciosos abram conexões para números de telefone pagos por minutos e caros.

Os programas de discador maliciosos podem tentar fechar sua conexão com a internet e abrir uma nova conexão discada para outro número. A conexão com este número pode ser muito cara e beneficiar o criador do programa de discador.

O uso do controle de discagem pode impedir que os programas de discador maliciosos fechem e abram novas conexões. O controle de discagem também impede que você disque acidentalmente os números errados ou caros. Verifique se as conexões discadas são seguras definindo:

- os números para os quais os programas podem abrir uma conexão discada e
- os programas que têm permissão para fechar as conexões discadas.

Nota: O controle de discagem é adequado para os usuários que usam um modem ou ISDN para conectar-se à internet.

A verificação de vírus e spyware reconhece os programas de discador maliciosos como spyware e pode removê-los do computador. Se um novo programa de discador malicioso não for reconhecido, o controle de discagem impede que esse programa de discador abra quaisquer conexões discadas.

Se você suspeitar que há um discador não reconhecido em seu computador, poderá enviar o arquivo do discador como uma amostra para o iG. Depois disso, o Oi atualizará o banco de dados de definições de vírus e spyware e você poderá verificar o computador novamente. O discador será então reconhecido e removido do computador.

121. O que fazer se uma janela pop-up do controle de discagem for exibida

Se a janela pop-up Nova tentativa de discagem for exibida, você poderá permitir ou negar a conexão discada.

Para permitir ou negar a conexão discada:

a) Verifique o nome do programa.

b) Verifique o número do telefone.

c) Permita ou negue a conexão discada:

- Se o número estiver correto (fornecido pelo seu provedor de serviços) e o programa for o que você mesmo abriu:
  - Selecione Lembrar desta decisão.
  - Clique em Permitir.
- Se o número estiver incorreto ou a conexão foi aberta automaticamente:
  - Selecione Lembrar desta decisão.
  - Clique em Negar.

A conexão será permitida ou negada com base na sua decisão. O número e as informações sobre o programa serão adicionados à lista de números na guia Lista de números . Depois de isso acontecer:

- Se você permitiu a conexão, nenhuma janela pop-up será mostrada se um programa tentar abrir uma conexão discada para este número novamente.
- Se você negou a conexão e um programa tentar abrir uma conexão discada para este número, a janela pop-up Tentativa de discagem negada será exibida. Feche a janela pop-up clicando em Fechar.

Nota: A janela pop-up Fechar Conexão pode ser exibida se um programa tentar fechar uma conexão discada. Se o programa for o que você mesmo fechou, permita que a conexão discada seja fechada. Você pode fazer isso clicando em Permitir. Se o programa não for o que você fechou, negue o fechamento clicando em Negar. Negar a tentativa de fechamento garante que nenhum programa de discador malicioso possa fechar a sua conexão com a Internet e abrir uma nova conexão para outro número.

122. Editar números de telefone permitidos

É possível adicionar números de telefone à lista na guia Lista de números para permitir ou negar conexões discadas para esses números.

Para adicionar um novo número à lista:

a) Na página principal, clique em Configurações.

b) Selecione Conexões de rede > Controle de discagem.

c) Clique na guia Lista de números.

d) Clique em Adicionar. A caixa de diálogo Acrescentar número/intervalo é aberta.

e) No campo Descrição, insira uma descrição para o número.

f) No campo Número, insira o número:

- Os seguintes caracteres podem ser usados: #*1234567890.
- Um código de área ou de país pode ser usado, por exemplo, 040-1234567, 00 358 9123 4567.
- Outros caracteres, como espaço e hífen, podem ser usados para agrupar os números. Porém, observe que o controle de discagem descarta os outros caracteres que não foram mencionados acima. Por exemplo, ele trata os números 09-1234567 como se fossem 091234567.
- Você pode inserir um intervalo de números usando os seguintes curingas:
  - O caractere "?" substitui qualquer número. Por exemplo, para negar a conexão discada para determinados números de serviços, insira 0900?234567.
  - O caractere "X" ou "x" substitui um ou vários números. Você pode usar esse curinga, por exemplo, para negar as conexões discadas internacionais. Se você geralmente usar "00" para fazer uma chamada internacional, insira "00x" para negar todas as conexões discadas internacionais.

g) Selecione se você deseja negar ou permitir as tentativas de conexão discada:

- Selecione Negado para bloquear todas as tentativas de conexão discada para o número inserido.
- Selecione Permitido para permitir conexões discadas no número inserido.

h) Clique em OK. A guia Lista de números agora mostra o número do telefone e o intervalo de números, e a ação que você selecionou:

- Se você permitiu o número, o ícone ✔ será mostrado na frente do número.
- Se você negou o número, o ícone ✖ será mostrado na frente do número.

i) Se for necessário alterar a ordem de prioridade dos números, clique no número dentro da lista que deseja mover e, com o botão do mouse pressionado, arraste o número para o novo local na tabela.

Nota: A guia Lista de números pode incluir alguns números predefinidos se o seu provedor de serviços negou ou permitiu conexões discadas para determinados números. Não é possível alterar ou remover esses números.

123. Ver programas que têm permissão para fechar conexões discadas

É possível exibir os programas que são seguros, que têm permissão para fechar as conexões discadas, na guia Configurações.

Essa guia mostra os seguintes programas:

- Os programas seguros que sempre têm permissão para fechar as conexões discadas, por exemplo, o navegador da web que você está usando.
- Os programas para os quais você é solicitado a optar por permitir ou negar o fechamento da conexão discada. A guia mostra os programas que têm permissão para fechar as conexões discadas.

Esta guia não mostra os programas bloqueados. Se você negou que um aplicativo encerrasse a conexão discada em uma janela pop-up, o aplicativo não consegue encerrar a conexão até você reiniciar o computador. Se você permitir que um aplicativo encerre a conexão discada, o aplicativo consegue encerrá-la a qualquer momento e você não tem de fazer a seleção novamente.

Para ver os programas:

a) Na página principal, clique em Configurações.
b) Selecione Conexões de rede > Controle de discagem.
c) Clique na guia Configurações. Essa guia mostra uma lista de programas que têm a permissão de fechar as conexões discadas.

124. Ver tentativas de conexão discada

Ao ativar o registro para o controle de discagem, você pode ver as tentativas de conexão discada que o produto detectou.

Por padrão, o registro do controle de discagem fica desativado.

Para ativar o registro:

a) Na página principal, clique em Configurações.
b) Selecione Conexões de rede > Controle de discagem.
c) Clique na guia Configurações.
d) Para ativar o registro, selecione Ativar registro de controle de discagem.
e) Para exibir o registro que foi criado, clique em Mostrar registro. É possível ver as seguintes informações:
   - Tentativas de abrir ou fechar as conexões discadas.

- Se as tentativas foram permitidas ou negadas.
- Números de telefone discados.

125. O que fazer se não conseguir acessar a internet

Se a conexão discada para o provedor de serviços da internet (ou para algum outro número de telefone) parar de funcionar, verifique se você não negou, sem intenção, conexões para aquele número.

Para fazer isso:

a) Na página principal, clique em Configurações.

b) Selecione Conexões de rede > Controle de discagem.

c) Clique na guia Lista de números.

d) Verifique se o número que você tentou discar está na lista. Se estiver e foi negado (o ícone ✖ é mostrado na sua frente), proceda da seguinte maneira:

- Selecione o número.
- Clique em Editar.
- Selecione Permitido.
- Clique em OK. O ícone em frente ao número foi alterado para ✔ .

Faça um teste para verificar se a conexão com o número está funcionando.

126. Onde encontrar alertas do firewall e arquivos de registro

Ao ver os alertas do firewall e os arquivos de registro, você pode descobrir como as conexões de rede são protegidas no seu computador.

127. Ver alertas do firewall

Você pode ver uma lista de todos os alertas do firewall gerados.

A lista contém alertas causados pelo firewall e pela prevenção contra intrusões.

Para exibir a lista:

a) Na página principal, clique em Configurações.

b) Selecione Conexões de rede > Firewall.

c) Clique na guia Regras.

d) Clique em Registro de alerta. A caixa de diálogo Alertas do firewall é aberta e mostra as seguintes informações:

Campo	Descrição
Hora	Hora do alerta.
Endereço remoto	O *Endereço IP* do computador do qual você recebeu tráfego ou para o qual enviou tráfego.
Ataq	Mostra quantas vezes um alerta semelhante foi gerado.
Descrição	Um texto de alerta foi adicionado para a *regra de firewall*. Se uma tentativa de invasão causou o alerta, o campo mostra as informações sobre o *padrão* da tentativa de invasão.

e) Para exibir os detalhes do alerta, selecione o alerta e clique em Detalhes.

f) Para mover para o alerta anterior ou para o próximo, clique no botão Voltar ou Avançar.

g) Após exibir os detalhes, clique em Fechar para fechar a caixa de diálogo de detalhes de Alertas do firewall.

h) Clique em Fechar para fechar a caixa de diálogo da lista de Alertas do firewall.

128. Informações sobre o alerta do firewall

Um alerta do firewall contém informações sobre o tráfego que causou o alerta.

Um alerta do firewall contém as seguintes informações:

Campo	Descrição
Descrição	Um texto de alerta foi adicionado à *regra de firewall*. Se o alerta for causado por uma tentativa de invasão, ele mostrará informações sobre o *padrão* da tentativa de invasão.
Ação	Mostra o que ocorreu, por exemplo, para o *firewall* bloquear ou permitir o tráfego.
Hora	A data e a hora em que o alerta foi gerado.
Direção	Mostra se o tráfego é de entrada ou de saída (de um computador remoto para o seu computador ou vice-versa).
Protocolo	O *protocolo IP* usado.
Serviços	Mostra os *serviços de firewall* com os quais este tráfego encontrou correspondência.
Endereço remoto	O *Endereço IP* do computador remoto.
Porta remota	A *porta* no computador remoto.

Campo	Descrição
Endereço local	O *Endereço IP* do seu computador.
Porta local	A *porta* no seu computador.

129. Ver o registro de ações

Se um programa, como um jogo de rede, não funcionar, verifique no registro de ações do controle de aplicativos se a conexão à internet foi negada ao programa.

O registro de ações é um arquivo de texto (action.log) que coleta automaticamente informações sobre as conexões de rede. O tamanho máximo do arquivo é 10MB. Depois que o arquivo se torna preenchido, as entradas do registro antigo são excluídas.

Para exibir o registro de ações:

a) Na página principal, clique em Configurações.

b) Selecione Conexões de rede > Início de sessão.

c) Clique em Registro de ações.

O registro de ações é aberto em um editor de texto ou visualizador padrão, por exemplo, no Bloco de Notas.

130. Exemplos de registro de ações

O registro de ações mostra informações sobre as conexões abertas e as alterações feitas na regra de firewall.

131. Abertura de uma conexão

Veja a seguir o exemplo de uma entrada no registro, que é criada quando o Internet Explorer é aberto e uma conexão a um servidor HTTP é estabelecida:

Data	Hora	Tipo	Motivo interno	Programa	Ação de controle	Ação de rede	*Protocolo*	*Endereço IP* remoto	*Porta* remota
2007-03-07	H13:07:15+02:00	informações	controle de aplicativos	C:\PROGRA~1\INTERN~1\iexplore.exe	permitir	conexão externa	6	10.0.1.14	80

132. Recebimento de uma conexão

Veja a seguir o exemplo de uma entrada no registro, que é criada quando um programa no computador está agindo como um *servidor* para outros computadores. Estes outros computadores podem conectar-se a este programa de *servidor* através da *porta* que o controle de aplicativos abriu no computador (*regra de firewall* dinâmica):

Data	Hora	Tipo	Motivo interno	Programa	Ação de controle	Ação de rede	*Protocolo*	*Endereço IP* remoto	*Porta* local
2007-03-04	H13:08:15+02:00	informações	controle de aplicativos	desconhecido	permitir	receber	17	10.0.1.146	138

133. Adição e remoção de uma regra de firewall dinâmica

Veja a seguir um exemplo de duas entradas no registro de uma *regra de firewall*:

- A primeira entrada mostra que o controle de aplicativos adicionou uma *regra de firewall* dinâmica. A regra permite uma conexão de entrada temporária para um programa.
- A segunda entrada mostra que o controle de aplicativos removeu a *regra de firewall* dinâmica e a conexão foi fechada.

Data	Hora	Tipo de alerta	Tipo de regra	Ação	Intervalo mínimo do endereço IP remoto	Intervalo máximo do endereço IP remoto	O intervalo de porta varia de	O intervalo de porta varia a	A porta local varia de	A porta local varia a	Ação de regra
2007-03-05	H13:06:59+02:00	informações	regra dinâmica	adicionado	0.0.0.0	255.255.255.0	0	65535	371	371	permitir
2007-03-05	H13:07:23+02:00	informações	regra dinâmica	removido	0.0.0.0	255.255.255.0	0	65535	371	371	permitir

134. Monitorar tráfego de rede com registro de pacote

Você pode iniciar o registro de pacotes para coletar informações sobre o tráfego de rede do IP.

135. Como funciona o registro de pacote

O registro de pacote coleta informações sobre o tráfego de rede IP.

Por padrão, o registro de pacote fica desativado. O registro de pacote é direcionado principalmente a usuários experientes que estão familiarizados com redes de computadores.

É possível ativar o registro de pacotes se você criou um conjunto de regras de firewall e deseja verificar como elas bloqueiam o tráfego. Você também pode fazer isso se suspeitar de atividades maliciosas na rede.

As informações são coletadas em 10 arquivos (packetlog.0-packetlog.9). Toda vez que você ativa o registro, o registro de pacotes é coletado em um novo arquivo. Depois que o décimo arquivo estiver cheio, o próximo registro será coletado novamente no primeiro arquivo. Dessa forma, você poderá exibir os registros anteriores enquanto um novo registro for gerado.

Além do tráfego do IP, o registro de pacotes também coleta informações sobre outros tipos de tráfego de rede, por exemplo, os protocolos necessários para a sua rede local. Estas informações incluem, por exemplo, roteamento.

O registro de pacotes tem o formato hexadecimal e suporta o formato tcpdump. Isso permite que você abra os arquivos de registro em um programa de registro de pacotes diferente do visualizador padrão do registro de pacotes. Você também pode usar um programa analisador de protocolo de rede para analisar o conteúdo mais detalhadamente.

136. Iniciar registro de pacote

Você pode iniciar o registro de pacote se suspeitar de atividades maliciosas na rede ou se, por exemplo, um jogo de rede parar de funcionar.

Para iniciar o registro:

a) Na página principal, clique em Configurações.

b) Selecione Conexões de rede > Início de sessão.

c) Use o tempo de registro e o tamanho de arquivo recomendados mostrados nos campos Tempo de registro e Máx arquivo registro . Caso deseje, você também poderá alterá-los.

d) Clique em Iniciar registro. Um novo arquivo será adicionado à lista de arquivos de registro. O tamanho do arquivo aumentará conforme as informações são coletadas no campo. Se a lista já contiver 10 arquivos de registro, o próximo registro será coletado em um campo já existente.

e) Para interromper o registro manualmente, clique em Concluir registro. O registro será interrompido automaticamente depois que o período de tempo de registro

definido expirar ou o tamanho máximo do arquivo de registro definido for alcançado.

Um novo arquivo de registro será gerado e adicionado à lista de arquivos de registro.

137. Ver o registro de pacote

Após ter gerado o registro de pacote, você poderá abri-lo para visualizá-lo.

Para ver o registro de pacote:

a) Na página principal, clique em Configurações.

b) Selecione Conexões de rede > Início de sessão.

c) Selecione o registro de pacote a ser exibido e clique em Detalhes. O visualizador de registro de pacote padrão abre. O painel superior da janela mostra todas as conexões estabelecidas.

Você pode exibir as seguintes informações:

Campo	Descrição
Horário	Horário em segundos a partir do momento que a sessão começou. Se o tempo da sessão for definido como 60 segundos, o horário inicial para o primeiro *pacote* é perto de 0 segundos e o horário inicial para o último *pacote* é perto de 60 segundos.
Ignorar (dir)	Mostra se o *firewall* permitiu acesso ou ignorou o *pacote* e mostra a direção do *pacote*: • Não: permitiu o *pacote*. • Sim: Ignorou o *pacote*. • Entrada: *Pacote* de entrada. • Saída: *Pacote* de saída Essas informações não estarão disponíveis se você exibir o arquivo em um programa de login de pacote que não seja o visualizador padrão do *registro de pacote*.
Protocolo	O *protocolo IP* usado.
Origem	*Endereço IP* de origem do *pacote*.
Destino	*Endereço IP* de destino do *pacote*.
ID	Informações do cabeçalho do *pacoteIP*: Identificador do pacote.
TTL	Informações do cabeçalho do *pacoteIP*: O valor de *Tempo de vida* do *pacote* define o número de dispositivos de rede pelos quais o *pacote* pode viajar antes de ser descartado.
Len	Informações do cabeçalho do *pacoteIP*: Duração total do *pacote*.
Descrição	Descrição do *pacote*.

O painel à direita mostra os tipos de tráfego e suas informações.

O painel inferior da janela mostra as informações em formato hexadecimal e ASCII.

Para exibir todos os tipos de tráfego de rede (não apenas o tráfego IP), desmarque a caixa de seleção Filtrar não IP.

138. Uso da internet com segurança

Os recursos descritos nessa seção ajudarão a utilizar a internet com segurança.

Proteção durante a navegação:

- Ajuda a navegar na internet com segurança fornecendo classificações de segurança de sites no navegador.
- Bloqueia o acesso a sites que foram classificados como perigosos.
- Fornece correções para vulnerabilidades conhecidas em programas instalados no computador.

Filtragem de e-mail:

- Bloqueia mensagens de e-mail com spam e phishing para que não cheguem à caixa de entrada.
- Possibilita permitir ou bloquear mensagens de e-mail de endereços de e-mail específicos.

139. O que é proteção durante a navegação

A proteção durante a navegação ajuda a avaliar a segurança dos sites visitados e evita que você acesse sites perigosos sem a intenção de acessá-los.

A proteção durante a navegação é um plug-in de navegador que mostra as classificações de segurança de sites listados em resultados de mecanismos de pesquisa e em conteúdo de e-mail da web. Ao ajudá-lo a evitar sites que contenham ameaças de segurança, como malware (vírus, worms, cavalos de tróia) e phishing, as classificações de segurança da proteção durante a navegação ajudam a evitar as últimas ameaças da internet que ainda não são reconhecidas pelos programas antivírus tradicionais.

Há quatro possíveis classificações de segurança para sites: seguro, suspeito, perigoso e desconhecido. Essas classificações de segurança são baseadas em informações de diversas fontes, como analistas de malware do Oi Antivírus Empresarial e parceiros, bem como classificações dadas por outros usuários da proteção durante a navegação.

A proteção durante a navegação também utiliza proteções contra vulnerabilidades, que são correções desenvolvidas pelo Oi para protegê-lo contra as vulnerabilidades encontradas em programas no seu computador. As proteções contra vulnerabilidades identificam os sites maliciosos e impedem que esses sites utilizem essas vulnerabilidades para, por exemplo, forçar um download não autorizado que contenha malware. As proteções contra vulnerabilidades não protegem você contra arquivos que você fez download intencionalmente e que podem conter malware; esse tipo de ameaça à segurança é coberto pela verificação de vírus e spyware.

140. Como ativar ou desativar a proteção durante a navegação

Você será impedido de acessar sites perigosos quando a proteção durante a navegação estiver ativada.

Para ativar ou desativar a proteção durante a navegação:

a) Na página principal, clique em Configurações.

b) Selecione Internet > Proteção durante a navegação.

c) Escolha uma das seguintes ações:

- Para ativar a proteção durante a navegação, selecione Ativar proteção durante a navegação.
- Para desativar a proteção durante a navegação, desmarque a opção Ativar proteção durante a navegação.

d) Clique em OK.

e) Se o seu navegador estiver aberto, reinicie-o para aplicar as configurações alteradas.

Dependendo da sua escolha, a proteção durante a navegação agora está ativada ou desativada.

141. Classificações de segurança da proteção durante a navegação

A proteção durante a navegação mostra as classificações de segurança de sites em resultados de mecanismos de pesquisa e no conteúdo do e-mail da web.

Os ícones codificados por cores mostram a classificação de segurança do site atual (na barra de ferramentas). A classificação de segurança de cada link nos resultados do mecanismo de pesquisa e nas mensagens do e-mail da web também é mostrada com os mesmos ícones. Quatro ícones codificados por cores são utilizados:

- Verde - mostra que a página é segura.
- Âmbar - mostra que a página é suspeita. A análise de segurança da página indica que ela é segura, mas muitos usuários deram a ela uma classificação de segurança baixa.
- Vermelho - mostra que a página é perigosa.
- Cinza - indica que a página não foi analisada e que nenhuma informação está disponível para ela no momento.

As classificações de segurança estão disponíveis nos seguintes sites de pesquisa:

- Google
- MSN Live
- Yahoo

É possível exibir classificações de segurança de links da web nos e-mails que você enviar e receber. As classificações de segurança estão disponíveis nos seguintes programas de e-mail:

- Google
- MSN Hotmail Classic
- Yahoo Mail

Dependendo das configurações de proteção durante a navegação, é possível visitar sites que tenham sido classificados como não seguros. Os sites são automaticamente bloqueados ou você é apenas notificado de um possível risco.

142. Mostrar classificações de links da web

As classificações da proteção durante a navegação podem ser mostradas para resultados de mecanismos de pesquisa, links no conteúdo do e-mail da web ou em ambos.

Para definir onde as classificações de proteção durante a navegação são mostradas:

a) Na página principal, clique em Configurações.
b) Selecione Internet > Proteção durante a navegação.
c) Selecione ou desmarque Resultados de mecanismos de pesquisa (Google, Yahoo etc.). Quando essa opção estiver selecionada, as classificações da proteção durante a navegação serão exibidas para os sites listados nos mecanismos de pesquisa (Google, Yahoo, etc.).
d) Selecione ou desmarque Link no webmail (Gmail, Yahoo Mail, Hotmail etc.). Quando essa opção estiver selecionada, as classificações da proteção durante a navegação serão exibidas para links no conteúdo das mensagens do webmail (Gmail, Yahoo, Hotmail, etc.).
e) Clique em OK.

As classificações de segurança serão exibidas de acordo com as configurações selecionadas.

Dica: É possível clicar em Resumo de segurança sobre esse site da web na janela pop-up de classificação de segurança para ir para o portal Proteção durante a navegação, onde encontrará mais detalhes sobre o site e os critérios em que a classificação de segurança dele está baseada.

143. Como classificar sites

É possível classificar como seguro ou perigoso qualquer site que você acessar.

Para classificar um site:

a) Clique em Relatório na barra de ferramentas. Essa ação abre a caixa de diálogo Avise-nos.
b) Selecione uma classificação para dar a sua opinião sobre a segurança do site (É seguro, Não é seguro ou Não tenho opinião).
c) Clique em OK. Essa ação abrirá a caixa de diálogo Obrigado pela notificação.

Dica: Selecione Não mostrar essa mensagem novamente se não desejar ver a caixa de diálogo de confirmação ao classificar sites no futuro.

d) Clique em OK.

A sua classificação agora é enviada para análise, e as informações de classificação são reunidas para este site.

144. Proteger contra conteúdo perigoso

A proteção durante a navegação bloqueia o acesso a sites não seguros com base nas configurações selecionadas.

Para selecionar quando bloquear o acesso a um site:

a) Na página principal, clique em Configurações.

b) Selecione Internet > Proteção durante a navegação.

c) Selecione ou desmarque as opções em Bloquear acesso quando:

- Selecione ou desmarque O site contém uma ameaça. Quando essa opção estiver selecionada, a proteção durante a navegação bloqueará o acesso a qualquer site que contenha vírus, spyware ou malware.
- Selecione ou desmarque O site é classificado como perigoso. Quando essa opção estiver selecionada, a proteção durante a navegação bloqueará o acesso a qualquer site que tenha sido classificado como perigoso pelo Oi Antivírus Empresarial.

d) Clique em OK.

Uma Página de bloqueio da proteção durante a navegação agora será aberta sempre que você navegar em um site que esteja bloqueado com base nas configurações selecionadas.

145. Permissão de acesso a sites confiáveis

Se a proteção durante a navegação bloquear o acesso a uma página que você confia e deseja acessar, será possível defini-la como um site confiável.

Para adicionar um site confiável:

a) Na página principal, clique em Configurações.

b) Selecione Internet > Proteção durante a navegação.

c) Clique em Sites confiáveis. A caixa de diálogo Sites confiáveis é aberta, exibindo uma lista de todos os sites adicionados como sites confiáveis.

d) Clique em Adicionar. Uma nova linha é exibida na lista.

e) Insira o endereço da web no campo Site:
   - Utilize o formato "www.exemplo.com/" para acessar esse site específico, mas bloquear o acesso, por exemplo, ao site "www.exemplo.com.br".
   - Utilize o formato "www.exemplo.com" para permitir acesso aos sites "www.exemplo.com" e "www.exemplo.com.br".

Nota: Utilize essa opção com cuidado porque ela define "www.exemplo.com" e "www.exemplo.com.br" como sites confiáveis. O último pode ser seguro, mas também pode ser um site falso que é utilizado para phishing.

f) Clique em OK. O endereço da web agora está incluído na lista Sites confiáveis.
g) Clique em OK.

O site não será mais bloqueado quando você tentar acessá-lo.

146. Ativar ou desativar as proteções contra vulnerabilidades

As proteções contra vulnerabilidades são correções para vulnerabilidades em programas instalados no seu computador e podem ser ativadas ou desativadas manualmente.

Para ativar ou desativar as proteções contra vulnerabilidades:

a) Na página principal, clique em Configurações.
b) Selecione Internet > Proteção durante a navegação.
c) Clique em Explorar proteções. A caixa de diálogo Proteções contra vulnerabilidades é aberta.
d) Selecione as proteções contra vulnerabilidades que você deseja ativar ou desativar na lista.
e) Clique em OK.

147. O que fazer quando um site estiver bloqueado

Uma página de bloqueio da proteção durante a navegação é exibida quando você tentar acessar um site que seja classificado como perigoso.

Quando uma página de bloqueio da proteção durante a navegação for exibida:

a) Clique em Ir para a página inicial para ir à página inicial sem acessar o site perigoso. Essa ação é altamente recomendável.

Dica: É possível clicar em Resumo de segurança deste site para ir para o portal Proteção durante a navegação, onde encontrará mais detalhes sobre o site e os critérios em que a classificação de segurança dele está baseada.

b) Se desejar entrar no site de qualquer maneira:
   - Selecione Nunca bloquear esse site se deseja evitar que esse site seja bloqueado no futuro e adicionar o site à lista de sites confiáveis, e, em seguida, clique em Desejo entrar no site assim mesmo.
   - Clique em Desejo entrar nesse site assim mesmo sem selecionar Nunca bloquear esse site para entrar no site bloqueado dessa vez (o site estará bloqueado no futuro).

148. Resumo de segurança de um site

Um resumo das informações de classificação de qualquer site classificado está disponível no portal Proteção durante a navegação.

O resumo de segurança de um site fornece mais detalhes sobre os critérios em que a classificação de segurança está baseada. Por exemplo, o resumo de segurança pode mostrar se a classificação de segurança está baseada no malware encontrado no site, em classificações baixas de outros usuários ou em ambos. O resumo de segurança pode ser acessado em diferentes lugares:

- No menu de classificação de segurança na barra de ferramentas,
- No pop-up de classificação de segurança de links de sites e
- No link de resumo de segurança em páginas de sites bloqueados pela proteção durante a navegação.

Clique em qualquer um desses links para ir para o portal Proteção durante a navegação, onde você verá os detalhes da classificação de segurança do site.

149. Bloquear spam

A filtragem de e-mail protege o computador contra mensagens de e-mail com spam e com phishing.

Uma mensagem de e-mail é considerada spam se for enviada como parte de uma coleção de mensagens, todas tendo conteúdo idêntico, e se os destinatários não concederam permissão para que a mensagem fosse enviada. As mensagens de spam e com phishing tendem a encher com frequência as mensagens de e-mail indesejadas. Você pode manter sua caixa de entrada livre de spam das seguintes maneiras:

- usar a filtragem de e-mail para capturar mensagens de spam e com phishing e para movê-las para as pastas de spam e phishing;
- bloquear mensagens de endereços de e-mail específicos adicionando-os à lista de remetentes bloqueados;
- permitir as mensagens provenientes de endereços de e-mail confiáveis adicionando-as à lista de remetentes seguros.

Se você utilizar uma lista de remetentes seguros, crie uma lista de contatos dos quais deseja receber mensagens de e-mail. Ao adicionar seus contatos a uma lista de remetentes seguros, você certifica-se de que as mensagens deles não serão movidas para as pastas de spam ou phishing.

Se você usar uma lista de remetentes bloqueados, você cria uma lista de remetentes dos quais você não deseja receber mensagens de e-mail. Ao adicionar remetentes a uma lista de remetentes bloqueados, você garante que suas mensagens sejam movidas para as pastas de spam ou phishing.

Nota: Se o endereço estiver também na lista de remetentes seguros, a mensagem de e-mail não será movida para a pasta de spam ou phishing porque a lista de remetentes seguros tem prioridade em relação à lista de remetentes bloqueados.

150. Configurar meus programas de e-mail para filtrar spam

É possível criar uma pasta de spam, de phishing e regras de filtragem em seu programa de e-mail para filtrar spam.

A filtragem de e-mail cria uma pasta de spam e de phishing e as regras de filtragem automaticamente no Microsoft Outlook, Microsoft Outlook Express e no Windows Mail (no Windows Vista). Se você usar algum outro programa de e-mail, deverá criar as pastas e as regras de filtragem manualmente. Se você tiver várias contas de e-mail, crie as regras de filtragem para cada conta separadamente.

Nota: A filtragem de spam e phishing suporta apenas o protocolo POP3. Os programas de e-mail baseados na web ou outros protocolos não são suportados.

151. Como as minhas próprias regras de filtragem e de e-mail funcionam juntas?

A filtragem de e-mail filtra as mensagens de e-mail com base nas suas próprias regras de filtragem. Ele não filtra mensagens de e-mail que correspondam a uma regra que você tenha criado. Se você criou, por exemplo, uma regra que filtra todas as mensagens de e-mail de um armazenamento da web para a pasta Armazenamento da web, tanto as mensagens de confirmação de ordem quanto o material de propaganda desse Armazenamento da web serão movidos da sua caixa de entrada e filtrados para a pasta Loja da web.

Esta seção contém instruções sobre como você pode criar a pasta de spam e a regra de filtragem para os programas de e-mail da Microsoft, Netscape, Mozilla Thunderbird e Eudora. Você também pode usar estas instruções para criar regras de filtragem semelhantes em outros programas de e-mail.

152. Programas de e-mail da Microsoft

A filtragem de e-mail cria pastas para mensagens de e-mail com spam e comphishing e as regras de filtragem automaticamente no Microsoft Outlook, Microsoft Outlook Express e Windows Mail (no Windows Vista).

153. Limpar as pastas de lixo e phishing

É possível configurar mensagens de e-mail spam e phishing, que são mais velhas do que o número definido de dias, para serem automaticamente excluídas no Microsoft Outlook, Microsoft Outlook Express e Windows Mail (no Windows Vista).

Se você estiver aguardando um e-mail e ele não estiver na caixa de entrada, verifique as pastas de lixo e phishing para certificar-se de que a mensagem não foi movida para essas pastas.

Para configurar as pastas lixo e phishing para serem automaticamente limpadas:

a) Na página principal, clique em Configurações.

b) Selecione Internet > Filtragem de e-mail.

c) Em Integração com o Outlook, proceda da seguinte maneira:

- Selecione Limpar as pastas de lixo após: [7] dias.

Selecione ou insira um número que determine que mensagens de e-mail deverão ser excluídas das pastas de lixo e phishing. Por exemplo, se você definir que as mensagens sejam excluídas das pastas após sete dias, o sistema excluirá automaticamente as mensagens com uma data de envio (no cabeçalho da mensagem) anterior há sete dias.

d) Clique em OK.

154. Programas de e-mail Netscape e Mozilla Thunderbird

Siga estas instruções para criar pastas para mensagens de e-mail com spam e phishing e regras de filtragem nos programas de e-mail Netscape e Mozilla Thunderbird.

155. Criar pastas para mensagens de e-mail com spam e phishing

É necessário criar pastas para mensagens de e-mail com spam e phishing manualmente nos programas de e-mail Netscape e Mozilla Thunderbird.

Para criar as pastas:

a) Selecione Arquivo > Novo > Pasta para criar uma nova pasta para mensagens de e-mail com spam.

b) Proceda da seguinte maneira:

- Insira spam como o nome da nova pasta.
- Na lista Criar como subpasta de, selecione o diretório no qual a sua caixa de entrada está localizada.

c) Clique em Ok para criar a nova pasta para spam.

d) Repita as etapas de 1a 3 para criar uma pasta para a qual as mensagens de e-mail com phishing serão filtradas.

e) Verifique se as novas pastas foram criadas e são exibidas em sua conta.

Após criar as pastas, crie regras de filtragem de spam e phishing.

156. Criar regra de filtragem de spam

Para filtrar as mensagens de e-mail spam para a pasta spam, é necessário criar uma regra de filtragem nos programas de e-mail do Netscape e do Mozilla Thunderbird.

Antes de criar uma regra de filtragem de spam, verifique se a pasta de spam existe.

Para criar a regra de filtragem de spam:

a) Selecione Ferramentas > Filtros de mensagens.

b) Clique em Novo. A caixa de diálogo Filtrar regras é exibida.

c) Insira spam como o nome da nova regra.

d) Crie uma nova entrada no cabeçalho, que será usada para filtrar as mensagens de e-mail com spam:
   - Selecione Personalizar na primeira lista.
   - Na caixa de diálogo Personalizar cabeçalhos, insira X-Spam-Flag como o novo cabeçalho da mensagem e clique em Adicionar.
   - Clique em OK.

e) Crie uma regra para mover uma mensagem de e-mail para a pasta de spam:
   - Na primeira lista, selecione X-Spam-Flag.
   - Na segunda lista, selecione contém.
   - Na caixa de texto, insira Yes como o texto para o qual você deseja achar correspondência.

f) Em Executar estas ações, proceda da seguinte maneira:
   - Na primeira lista, selecione Mover mensagem para.
   - Na segunda lista, selecione a pasta de spam que você criou anteriormente.

g) Clique em OK para confirmar a sua nova regra de filtragem de spam e para fechar a caixa de diálogo Regras de filtragem.

h) Feche a caixa de diálogo Filtros de mensagens.

Você criou a regra de filtragem de spam. De agora em diante, as mensagens de e-mail com spam serão filtradas para a pasta de spam.

157. Criar regra de filtragem de phishing

Para filtrar mensagens de e-mail com phishing, é necessário criar uma regra de filtragem nos programas de e-mail Netscape e Mozilla Thunderbird.

Antes de criar uma regra de filtragem de phishing, verifique se a pasta para a qual as mensagens de e-mail com phishing podem ser filtradas existe.

Para criar a regra de filtragem de phishing:

a) Selecione Ferramentas > Filtros de mensagens.

b) Clique em Novo. A caixa de diálogo Filtrar regras é exibida.

c) Insira phishing como o nome do novo filtro.

d) Crie uma nova entrada de cabeçalho, que é usada para filtrar as mensagens de e-mail com phishing:
   - Selecione Personalizar na primeira lista.
   - Na caixa de diálogo Personalizar cabeçalhos, insira X-FS-Classification-Phishing como o novo cabeçalho da mensagem e clique em Adicionar.
   - Clique em OK.

e) Crie uma regra para mover uma mensagem de e-mail para a pasta de phishing:
   - Na primeira lista, selecione X-FS-Classification-Phishing.
   - Na segunda lista, selecione contém.
   - Na caixa de texto, digite 9 como o texto para o qual você deseja encontrar uma correspondência.

f) Em Executar estas ações, proceda da seguinte maneira:
   - Na primeira lista, selecione Mover mensagem para.
   - Na segunda lista, selecione a pasta de phishing criada previamente.

g) Clique em OK para confirmar a sua nova regra de filtragem de phishing e para fechar a caixa de diálogo Regras de filtragem.

h) Feche a caixa de diálogo Filtros de mensagens.

A regra de filtragem de phishing foi criada. De agora em diante, as mensagem de e-mail com phishing serão filtradas para a pasta para phishing.

158. Programa de e-mail Opera

Siga estas instruções para criar pastas de mensagens de e-mail com spam e phishing e regras de filtragem no programa de e-mail Opera.

159. Criar filtros para mensagens de e-mail com spam e phishing

A filtragem de e-mail cria o filtro de spam automaticamente no programa de e-mail Opera.

É necessário criar um filtro de phishing manualmente.

Nota: Os filtros de spam e phishing no Opera são equivalentes às pastas criadas para mensagens de e-mail com spam e phishing em outros programas de e-mail.

Para criar um filtro de phishing:

a) Abra a exibição do Opera Mail.

b) No painel E-mail, clique com o botão direito do mouse em Todas as mensagens e selecione Novo filtro.

c) Insira um nome para o filtro de phishing. O novo filtro é mostrado em Filtros no painel do e-mail.

d) Verifique se os novos filtros de spam e phishing foram criados e são mostrados em Filtros.

Após criar o filtro para as mensagens de e-mail com phishing, crie regras de filtragem de spam e phishing.

160. Criar regra de filtragem de spam

Para filtrar mensagens de e-mail com spam, é necessário criar uma regra de filtragem no programa de e-mail Opera.

Antes de criar uma regra de filtragem de spam, verifique se o filtro de spam existe.

Nota: As etapas fornecidas aqui aplicam-se ao Opera versão 9.6. As etapas para as outras versões podem variar um pouco.

Para criar uma regra de filtragem de spam:

a) Abra a exibição Opera Mail.

b) Clique com o botão direito do mouse no filtro de spam e selecione Propriedades.

c) Selecione a regra padrão exibida na lista. Se a lista não contiver nenhuma regra, clique em Adicionar regra.

d) Crie uma regra para mover uma mensagem de e-mail para o filtro de spam:
   - Na primeira lista, selecione qualquer cabeçalho.
   - Na segunda lista, selecione contém.
   - Na caixa de texto, insira X-Spam-Flag: Sim como o texto para o qual você deseja achar correspondência.

Certifique-se de deixar espaço entre os dois pontos e Yes.

e) Clique em OK para confirmar a sua nova regra de filtragem de spam.

161. Criar regra de filtragem de phishing

Para filtrar mensagens de e-mail com phishing, é necessário criar uma regra de filtragem no programa de e-mail Opera.

Antes de criar uma regra de filtragem de phishing, verifique se a pasta para a qual as mensagens de e-mail de phishing podem ser filtradas existe.

Nota: As etapas fornecidas aqui aplicam-se ao Opera versão 9.6. As etapas para as outras versões podem variar um pouco.

Para criar uma regra de filtragem de phishing:

a) Abra a exibição Opera Mail.

b) Clique com o botão direito do mouse no filtro de phishing e selecione Propriedades.

c) Selecione a regra padrão exibida na lista. Se a lista não contiver nenhuma regra, clique em Adicionar regra.

d) Crie uma regra para mover uma mensagem de e-mail para o filtro phishing:
   - Na primeira lista, selecione qualquer cabeçalho.
   - Na segunda lista, selecione contém.
   - Na caixa de texto, insira X-FS-Classification-Phishing: 9 como o texto para o qual você deseja achar uma correspondência.

Certifique-se de deixar espaço entre os dois pontos e o '9'.

e) Clique em OK para confirmar a sua nova regra de filtragem de phishing.

162. Programa de e-mail Eudora

Siga estas instruções para criar pastas de mensagens e-mail, spam e phishing e regras de filtragem no programa de e-mail Eudora.

163. Criar pastas para mensagens de e-mail com spam e phishing

É necessário criar uma pasta para spam manualmente no programa de e-mail Eudora.

Para criar uma pasta para spam:

f) Selecione Caixa de correio > Novo.

g) Nomeie a nova caixa de correio de spam.

h) Repita as etapas de 1a 2 para criar uma pasta para a qual as mensagens de e-mail com phishing possam ser filtradas.

i) Verifique se as novas pastas foram criadas e são exibidas nas caixas de correio do Eudora.

Após criar as pastas, crie as regras de filtragem de spam e phishing.

164. Criar regra de filtragem de spam

Para filtrar mensagens de e-mail com spam, é necessário criar uma regra de filtragem no programa de e-mail Eudora.

Antes de criar uma regra de filtragem, verifique se a pasta de spam existe.

Para criar uma regra de filtragem de spam:

a) Selecione Ferramentas > Filtros.

b) Clique em Novo.

c) Em Corresponder, selecione Recebida para filtrar as mensagens de e-mail recebidas.

d) Crie uma regra para mover uma mensagem de e-mail para a pasta de spam:

- Na lista Cabeçalho, insira X-Spam-Flag no campo Cabeçalho.
- Na segunda lista, selecione contém.
- Insira Yes no campo contém.

e) Em Ação, proceda da seguinte maneira:

- Na primeira lista, selecione Transferir para.
- Clique em Em e na lista, selecione a caixa de correio de spam.

f) Feche a caixa de diálogo Filtros.

g) Clique em Sim para salvar as alterações.

165. Criar regra de filtragem de phishing

Para filtrar mensagens de e-mail com phishing, é necessário criar uma regra de filtragem no programa de e-mail Eudora.

Antes de criar uma regra de filtragem de phishing, verifique se a pasta para a qual as mensagens de e-mail de phishing podem ser filtradas existe.

Para criar uma regra de filtragem de phishing:

a) Selecione Ferramentas > Filtros.

b) Clique em Novo.

c) Em Corresponder, selecione Recebida para filtrar as mensagens de e-mail recebidas.

d) Crie uma regra para mover uma mensagem de e-mail para a pasta phishing:
   - Na lista Cabeçalho, digite X-FS-Classification-Phishing no campo Cabeçalho
   - Na segunda lista, selecione contém.
   - Insira 9 no campo contém.

e) Em Ação, proceda da seguinte maneira:
   - Na primeira lista, selecione Transferir para.
   - Clique em "Em" e na lista, selecione a caixa de correio de phishing.

f) Feche a caixa de diálogo Filtros.

g) Clique em Sim para salvar as alterações.

166. E se eu receber um monte de spam

Se você receber muitas mensagens de e-mail com spam em sua caixa de entrada, há algumas configurações que podem ser verificadas.

Para reduzir a quantidade de mensagens de e-mail com spam recebidas, proceda da seguinte maneira:

a) Verifique se filtragem de e-mail está ativada:
   - Na página principal, clique em Configurações.
   - Selecione Internet > Filtragem de e-mail.
   - Selecione Ativar filtragem de e-mail, se já não estiver selecionada.

b) Verifique se criou pastas para spam e phishing e regras de filtragem em seu programa de e-mail.

c) Em seu programa de e-mail, verifique se o protocolo POP3 está selecionado. A filtragem de e-mail suporta apenas o protocolo POP3. Para obter orientações sobre a verificação do protocolo, consulte o provedor de serviços de internet.

d) Verifique se a filtragem de e-mail monitora a mesma porta que o seu programa de e-mail. Você só precisa alterar a porta se o seu programa de e-mail usar uma porta que não seja padrão.

- Na página principal, clique em Configurações.
- Selecione Internet > Verificação de vírus e spyware.
- Clique em Protocolos.
- Em Números de porta, verifique se o número da porta usado para o protocolo POP3 é o mesmo que o da porta usada no seu programa de e-mail. Para obter informações sobre a porta usada para o protocolo POP3, consulte o seu provedor de serviços da internet.
- Clique em OK.
- Verifique se o seu nível de filtragem é restrito o suficiente:
- Na página principal, clique em Configurações.
- Selecione Internet > Filtragem de e-mail.
- Em Modo de filtragem de spam e phishing, selecione Agressivo, se já não estiver selecionado.
- Clique em OK.

167. Quais são os níveis de spam e phishing

Os níveis de filtragem de spam determinam com que agressividade a filtragem de e-mail bloqueia as mensagens de e-mail com spam e com phishing.

Quando a filtragem de e-mail detectar mensagens de e-mail com spam ou com phishing, ela as moverá para uma pasta especial de spam ou phishing, de acordo com o nível de filtragem selecionado. Se você achar que recebe mensagens de e-mail com spam demais em sua caixa de entrada, selecione um nível de filtragem mais rígido. Se acha que vários e-mails legítimos estão sendo bloqueados pelo filtro, selecione um nível menos rígido.

É possível selecionar os seguintes níveis predefinidos:

- Agressivo - selecione esse nível se você receber muitas mensagens com spam e desejar bloquear o máximo possível.
- Médio - (configuração padrão) selecione esse nível se você não receber muitas mensagens de e-mail com spam ou se as mensagens de e-mail legítimas enviadas para você não forem filtradas como spam.

168. Alterar o nível de filtragem de spam e phishing

Ao selecionar um nível de filtragem mais agressivo, você pode reduzir o número de mensagens de e-mail com spam que você recebe na sua caixa de entrada.

Para alterar o nível de filtragem:

a) Na página principal, clique em Configurações.

b) Selecione Internet > Filtragem de e-mail.

c) Em Modo de filtragem de spam e phishing, selecione um dos níveis de filtragem predefinidos.

d) Clique em OK.

169. Redefinir sistema de aprendizagem de spam e phishing

Quando a filtragem de e-mail verifica as mensagens, ela automaticamente aprende a reconhecer as mensagens com spam e com phishing com mais precisão.

Nota: Redefina o sistema de aprendizagem somente se você for instruído a fazê-lo.

Às vezes há problemas no processo de aprendizagem. Consequentemente, os e-mails legítimos poderão ser detectados como spam ou phishing. É possível redefinir o sistema de aprendizagem para limpar as regras aprendidas.

Para restaurar as configurações padrão:

a) Na página principal, clique em Configurações.

b) Selecione Internet > Filtragem de e-mail.

c) Clique em Redefinir filtros.

d) Na mensagem de confirmação, clique em OK.

O sistema de aprendizagem é redefinido e o sistema usa as configurações padrão.

170. Definir a porta para protocolos de e-mail

Se o seu programa de e-mail usa uma porta que não seja padrão, você deve alterar a porta que é verificada para encontrar spam.

Para definir a porta:

a) Abra o aplicativo de e-mail e verifique que porta está sendo usada para receber e-mails POP3. Anote o número da porta.

Nota: Protocolos de e-mail que não sejam POP3 não são suportados.

b) Abra o produto.

c) Na página principal, clique em Configurações.

d) Selecione Internet > Filtragem de e-mail.

e) Clique em Mostrar protocolos.

f) Insira o número da porta usada pelo protocolo de e-mail POP3.

g) Clique em OK.

171. Permitir e bloquear mensagens de endereços de e-mail específicos

É possível usar listas de remetentes seguros e bloqueados para permitir e bloquear mensagens de e-mail provenientes de endereços de e-mail específicos.

Uma lista de remetentes bloqueados e seguros ajuda você a bloquear mensagens de e-mail indesejadas e a permitir o envio de outras. Uma lista de remetentes seguros reduz o número de mensagens de e-mail legítimas que são identificadas incorretamente como mensagens de e-mail com spam ou com phishing.

172. Editar endereços de e-mail em que confio

Ao adicionar endereços de e-mail à sua lista de remetentes seguros, você certifica-se de que as mensagens de e-mail advindas desses endereços são permitidas e nunca são tratadas como spam ou phishing.

É possível adicionar, editar ou remover endereços de e-mail individuais ou domínios inteiros da lista de remetentes permitidos. Por exemplo, se você adicionar *@exemplo.com à lista de remetentes permitidos, todas as mensagens de e-mail provenientes do domínio exemplo.com serão permitidas.

Para editar a lista de endereços de e-mail confiáveis:

a) Na página principal, clique em Configurações.

b) Selecione Internet > Filtragem de e-mail.

c) Clique em Permitir remetentes. A página de configurações Remetentes de e-mail permitidos é aberta.

d) Escolha uma das seguintes ações:

- Para adicionar um novo endereço de e-mail:
  - Clique em Adicionar. A caixa de diálogo Editar Remetente/Domínio é aberta.
  - No campo Endereço, insira o endereço de e-mail ou nome de domínio do qual você deseja permitir mensagens de e-mail. É possível adicionar uma breve descrição do novo endereço no campo Descrição.
  - Clique em OK. O novo endereço de e-mail agora é mostrado na lista de remetentes seguros.
- Para editar um endereço de e-mail:
  - Na lista, selecione o endereço de e-mail a ser editado e clique em Editar. A caixa de diálogo Editar Remetente/Domínio é aberta.
  - Edite o endereço de e-mail selecionado e clique em OK.
  - Para remover um endereço de e-mail da lista de remetentes permitidos:
  - Na lista, selecione o endereço de e-mail que você deseja remover e clique em Remover. O endereço de e-mail é removido da lista.

173. Importar contatos para a minha lista de remetentes seguros

É possível importar contatos de catálogos de endereços do Microsoft Outlook, Microsoft Outlook Express e do Windows Mail (no Windows Vista) para a lista de remetentes seguros.

Ao importar contatos para a lista de remetentes seguros, você certifica-se de que as mensagens de e-mail provenientes desses endereços de e-mail não sejam filtradas incorretamente como mensagens de e-mail com spam ou phishing.

Para importar contatos:

a) Na página principal, clique em Configurações.

b) Selecione Internet > Filtragem de e-mail.

c) Clique em Permitir remetentes. A página Remetentes de e-mail permitidos é aberta.

d) Clique em Importar contatos do Outlook. É exibida uma mensagem informando se a importação dos contatos foi bem-sucedida ou não.

Nota: Se houve falha na importação de contatos, a mensagem mostrará o motivo.

e) Clique em OK para fechar a mensagem.

f) Clique em OK.

Os contatos importados agora são mostrados na lista de remetentes seguros.

174. Bloquear mensagens de endereços de e-mail específicos

Mensagens de e-mail dos domínios ou endereços da sua listas de remetentes bloqueados são tratadas como spam ou phishing e filtradas para a pasta spam ou phishing.

É possível adicionar, editar ou remover endereços de e-mail individuais ou domínios inteiros da sua lista de remetentes bloqueados. Por exemplo, se adicionar *@example.com à sua lista de remetentes bloqueados, todas as mensagens de e-mail do domínio example.com serão bloqueadas.

Para editar a lista de endereços de e-mail bloqueados:

a) Na página principal, clique em Configurações.

b) Selecione Internet > Filtragem de e-mail.

c) Clique em Bloquear remetentes.

d) Escolha uma das seguintes ações:

- Para adicionar um novo endereço de e-mail:
  - Clique em Adicionar. A caixa de diálogo Editar Remetente/Domínio é aberta.
  - No campo Endereço, insira o endereço de e-mail ou nome de domínio do qual você deseja bloquear mensagens de e-mail. É possível adicionar uma breve descrição do novo endereço no campo Descrição.
  - Clique em OK. O novo endereço de e-mail agora é mostrado na lista de remetentes bloqueados.

- Para editar um endereço de e-mail:
  - Na lista, selecione o endereço de e-mail a ser editado e clique em Editar. A caixa de diálogo Editar Remetente/Domínio é aberta.
  - Edite o endereço de e-mail selecionado e clique em OK.
  - Para remover um endereço de e-mail da lista de remetentes bloqueados:
  - Na lista, selecione o endereço de e-mail que você deseja remover e clique em Remover. O endereço de e-mail é removido da lista.

175. Proteger contra tentativas de phishing

A filtragem de e-mail protege o seu computador contra tentativas de phishing que utilizam mensagens de e-mail falsas, que parecem vir de negócios legítimos, para roubar informações pessoais.

Essas mensagens falsamente autênticas foram criadas para fazer com que você forneça dados pessoais, tais como número de conta de banco, senhas, cartão de crédito e número do seguro social. Não confie em nenhuma mensagem de e-mail assinalada como Phishing.

Quando você receber uma nova mensagem de e-mail identificada como uma tentativa de phishing, ela será movida automaticamente para a pasta de phishing.

No Microsoft Outlook, Outlook Express e Windows Mail (no Windows Vista), a pasta e a regra phishing são criadas automaticamente. Se você usar outro programa de e-mail, crie a pasta e a regra de filtragem de phishing manualmente.

Neste produto, o Anti-Phishing faz parte da filtragem de e-mail.